ELECTRICITY INFRASTRUCTURE THREATS AND POLICY RESPONSE

A Dissertation
Presented to
The Academic Faculty

By

Jenna K.C. McGrath

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy in the
School to Public Policy

Georgia Institute of Technology

December 2018

COPYRIGHT © 2018 BY JENNA K.C. MCGRATH

ELECTRICITY INFRASTRUCTURE THREATS AND POLICY RESPONSE

Approved By:

Dr. Valerie Thomas, Advisor
School of Industrial and Systems Engineering - School of Public Policy
Georgia Institute of Technology

Dr. Marilyn Brown
School of Public Policy
Georgia Institute of Technology

Dr. Margaret Kosal
Sam Nunn School of International Affairs
Georgia Institute of Technology

Dr. Daniel Matisoff
School of Public Policy
Georgia Institute of Technology

Dr. Juan Moreno-Cruz
School of Environment, Enterprise and Development
University of Waterloo

Date Approved: October 23, 2018

AKNOWLEDGEMENTS

I am sincerely grateful for the unwavering encouragement, patience, and support I received from my parents, my sister, Christopher, and the dear friends I have made through this journey.

Thank you to my advisor, Dr. Valerie Thomas, for her support, motivation, and positive outlook throughout this process. Further thanks to my committee members, Drs. Marilyn Brown, Margaret Kosal, Juan Moreno-Cruz, and Dan Matisoff. I am appreciative of the resources and opportunities I have had to conduct my research and explore new ideas, particularly through the Climate and Energy Policy Laboratory, the NSF IGERT program, the Sam Nunn Security Program, the Strategic Energy Institute, the Institute for Information Security and Privacy, and the Global Security Program at Lawrence Livermore National Laboratory.

TABLE OF CONTENTS

AKNOWLEDGEMENTS ..... **iii**

LIST OF TABLES ..... **vii**

LIST OF FIGURES ..... **viii**

LIST OF ABBREVIATIONS ..... **x**

SUMMARY ..... **xi**

CHAPTER 1. INTRODUCTION **1**

1.1 Targeted Attacks Against U.S. Electricity Infrastructure 2

1.2 Federal R&D Funding Response to Incidents on the Electric Grid 4

1.3 Will Updated Electricity Infrastructure Security Protect the Grid? 8

1.4 Public and Private Response to Incidents Impacting Critical Infrastructure 10

CHAPTER 2. TARGETED ATTACKS AGAINST U.S. ELECTRICITY INFRASTRUCTURE **12**

2.1 Introduction 12

2.2 Critical Infrastructure as a Target 15

2.3 Vulnerability of the Electrical Infrastructure 16

2.4 Databases and Research on Critical Infrastructure Attacks 19

2.5 Data & Methodology 22

2.5.1 Exclusions: 24

2.6 Motives and Intent for Attacks 26

2.6.1 Attacks in Protest or Reaction to a Single Focusing Event 28

2.6.2 Attacks Aimed at Disrupting Government, Economy, or Utility 29

2.6.3 Attacks Motivated by Environmental Factors 32

2.6.4 Attacks in Protest Against U.S. Foreign or Military Policy 33

2.6.5 Attacks as an Act of Vandalism 34

2.6.6 Incidents as an Act of Theft 35

2.6.7 Attacks as an Act of Sabotage Not Otherwise Specified 35

2.7 Results 36

2.8 Discussion 42

2.8.1 The Emerging Subset of Sophisticated and/or Coordinated Attacks 46

2.9 Conclusions & Recommendations 50

CHAPTER 3. FEDERAL R&D FUNDING RESPONSE TO INCIDENTS ON THE ELECTRIC GRID 54

3.1 Introduction 54

3.2 Background 55

3.3 Risk Perception Theory and Hypotheses 58

3.4 Data and Methodology 61

3.4.1 Disturbance Database Description 61

3.4.2 Office of Electricity Funding Allocations Description 66

3.4.3 Committee Report Description 69

3.5 Methodology 71

3.6 Results 77

3.7 Discussion 80

3.8 Conclusions & Implications for Future Research 83

CHAPTER 4. WILL UPDATED ELECTRICITY INFRASTRUCTURE SECURITY PROTECT THE GRID? A CASE STUDY MODELING ELECTRICAL SUBSTATION ATTACKS 85

4.1 Introduction 85

4.2 Background 86

4.2.1 Metcalf Attack and Utility-Level Security Improvements 88

4.2.2 NERC-Level Security Improvements 90

4.3 Data and Methodology 92

4.3.1 JCATS MODELING 92

4.3.2 Security Upgrade Levels 94

4.4 Attacker Profiles 97

4.5 Attack Scenarios 99

4.6 Results 102

4.6.1 Physical Attacks 102

4.6.2 Cyber-Enabled Physical Attacks 108

4.7 Discussion 110

4.8 Conclusions 113

CHAPTER 5. PUBLIC AND PRIVATE RESPONSE TO INCIDENTS IMPACTING CRITICAL INFRASTRUCTURE 116

5.1 Introduction 116

5.2 Background 119

5.2.1 Disaster Response 119

5.3 Utilizing Power-Law Scaling Relationships to Evaluate Incident Impact 121

5.4 Data and Methodology 124
5.4.1 Data Selection 125
5.4.2 Monetarization of Human Health Impact 127
5.5 Results and Analysis 133
5.6 Discussion 141
5.7 Conclusion and Implications for Future Research 145
CHAPTER 6. CONCLUSION 147
6.1 Targeted Attacks Against U.S. Electricity Infrastructure 148
6.2 Federal R&D Funding Response to Incidents on the Grid 149
6.3 Will Updated Electricity Infrastructure Security Protect The Grid? 150
6.4 Public And Private Response To Incidents Impacting Critical Infrastructure 151
6.5 Future Outlook 151
APPENDIX 154
REFERENCES 157

LIST OF TABLES

Table 3-1. Total Keyword Count from Energy and Water Development Appropriations Committee Reports, 2003-2018 *Includes Committee Reports for Energy Policy Act **Includes Committee Reports for American Recovery and Reinvestment Act 73
Table 3-2. Summary Statistics of U.S. Electricity Disturbance Database (2000 to 2017) and Department of Energy Fiscal Year Funding (2003-2017) 75
Table 3-3. Mediation Hypothesis Model Results for Hypotheses 1, 2, and 3, time lag 1 year. 78
Table 4-1. Security Upgrade Scenarios (laboratory-specific reference number LLNL-TR-746040). 95
Table 4-2. Attacker Profiles, LLNL-TR-746040. 99
Table 4-3. Attack Scenario Details. 101
Table 4-4. Physical Attack Scenario Results, LLNL-TR-746040. 105
Table 4-5. Security Upgrade 4: Cyber-Enabled Attack 109
Table 5-1. Significant Events Across Critical Infrastructure Sectors *N/A indicates information is not available for incidents where if were either no injuries or injuries were not reported. 123
Table 5-2. Agency-Specific Values of Statistical Life, in constant 2017 millions of dollars, used to estimate Human Health Impact (Merrill, 2017) 128
Table 5-3. Severity of Injury Human Health Impact monetary estimate, where cost is based on project 2020 Income Levels (Office of Air and Radiation, 2011) 129
Table 5-4. Monetary Impact, Response, and Insured Losses associated with major incidents impacting the critical infrastructure sectors. All values are in constant 2017 millions dollars. 130
Table 5-5. The total Impact, Total Public Response, and Total Public and Private Responses (Total Public Response plus insured losses. All values in constant 2017 millions of dollars. **Insured Losses Represents the Private Sector's Response... 132

LIST OF FIGURES

Figure 1-1. Risk Perception Process....6
Figure 2-1. Total attacks on the grid, 1970-2016....39
Figure 2-2. Targets of attack on the electric grid, 1970-2016....39
Figure 2-3. Attack methods used to target the electric grid, 1970-2016....40
Figure 2-4. Motives for attacking the electric grid, 1970-2016....40
Figure 2-5. Motives for attacking the grid, 1970-1999....41
Figure 2-6. Motives for attacking the grid, 2000-2016....41
Figure 2-7. Sophisticated and/or coordinated attacks on the grid, 1970-2016....47
Figure 3-1. Risk Perception Process. Do risks predict Congressional discussion, which in turn predicts funding response?....60
Figure 3-2. Total Number of Disturbances on the U.S. Grid, 2000-2017....64
Figure 3-3. Total Number of Disturbances on the U.S. Grid per year, 2000-2017....65
Figure 3-4. Total Number of Disturbances Caused by Malicious Events on the U.S. Grid per year, 2000-2017....66
Figure 3-5. DOE & DOE Office of Electricity and Energy Reliability R&D Fiscal Year Budgets, in Millions $2018 **Discretionary budgets, include non-R&D components **Latest estimates, FY 2017 is the President's request (AAAS, 2018).....69
Figure 4-1. Baseline Model of Substation in JCATS, LLNL-PRES-746039.....103
Figure 4-2. Damaged or Destroyed Transformers from a physical attack, based on Security Upgrade Level....107
Figure 4-3. Damaged or Destroyed Targets in Cyber-Enabled Physical Attacks....110
Figure 4-4. Elite Attackers (red) in a Cyber-Enabled Physical Attack, LLNL-PRES-746039....111
Figure 5-1. Human Health Impact ($M) and the Total Public Response (FEMA & Other) Allocated ($M) for major incidents impacting critical infrastructure. 134
Figure 5-2. Immediate Cost Impact ($M) and the Total Public Response (FEMA & Other)....135

Figure 5-3. Total Impact (Human Health and Cost) ($M) and the Total Public Response (FEMA and Other Federal or State responses) ($M) for major incidents impacting critical infrastructure. 136
Figure 5-4. Human Health Impact ($M) and Insured Loss ($M) associated with major incidents impacting critical infrastructure. 137
Figure 5-5. Immediate Costs ($) and Insured Loss ($M) associated with major incidents impacting critical infrastructure. 138
Figure 5-6. Human Health Impacts ($M) and Total Public and Private Response (FEMA and Other Federal or State funding responses, plus Insured Losses) Allocated ($M) for major incidents impacting critical infrastructure. 139
Figure 5-7. Immediate cost impacts and the Total Public and Private Response (FEMA and Other Federal or State funding responses, plus Insured Losses) Allocated ($M) for major incidents impacting critical infrastructure. 140
Figure 5-8. Total Impact (Human Health plus Cost) ($M) and the Total Public and Private Response (FEMA and Other Federal or State funding responses, plus Insured Losses) Allocated ($M) for major incidents impacting critical infrastructure. 141
Figure A-0-1. Human Health Impact ($M) compared with both FEMA Response ($M) and Other Federal or State Responses ($M).....155
Figure A-0-2. Immediate Costs ($M) compared with both FEMA Response ($M) and Other Federal or State Responses ($M).....156

LIST OF ABBREVIATIONS

AAAS	American Association for the Advancement of Science
AMSAA	Army Materiel Systems Analysis Activity
AP	Associated Press
ARPA-E	Advanced Research Projects Agency – Energy
ARRA	American Recovery and Reinvestment Act
CESER	Cyber Security, Energy Security, and Emergency Response
CIA	Central Intelligence Agency
CIP	Critical Infrastructure Protection
DOE	Department of Energy
DHS	Department of Homeland Security
DOT	Department of Transportation
E-ISAC	Electric Information Sharing and Analysis Center
EPA	Environmental Protection Agency
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FEMA	Federal Emergency Management Agency
GDT	Global Terrorism Database
GW	Gigawatt
HHI	Human Health Impacts
HHS	Health and Human Services
IC	Immediate Costs
IED	Improvised Explosive Devices
JCATS	Joint Conflict and Tactical Simulation
kV	kilovolt
LLNL	Lawrence Livermore National Laboratory
NERC	North American Electricity Reliability Corporation
NWLF	New World Liberation Front
OE	Office of Electricity Delivery and Energy Reliability
OLS	Ordinary Least Squares
PG&E	Pacific Gas and Electric
PLOSB	Probability Line-Of-Site Blocked
PSAT	Physical Security Analysis Team
PSAG	Physical Security Advisory Group
R&D	Research and Development
START	Terrorism and Response to Terrorism (database)
U.S.	United States
VSL	Value of a Statistical Life
WTP	Willingness-To-Pay

SUMMARY

The overarching research question of this dissertation is how are policymakers responding to threats to the electricity grid? The database of attacks on the United States electricity system, created and analyzed in Chapter 2, underscores that targeted attacks have been a persistent threat for the electric grid for the past nearly 50 years. In recent years, attacks have become more sophisticated and coordinated. Given this development, Chapter 3 considers how policy makers have responded to grid attacks, focusing on a more recent timeframe of seventeen years and uses risk perception theory as a guide. The results of the regression time series analysis indicate that policymakers respond to malicious attacks on the grid in terms of federal funding and allocation to grid-related improvements. There is no response associated with disruptions caused by severe weather or human or technical failures. This suggests that policymakers are perceiving malicious attacks as a threat and are stating policy priorities to address this issue in the federal budget appropriations.

In addition to funding for emergency response and funding for research, federal policy, utilities have proposed measures to improve grid security. Chapter 4 addresses the adequacy of this response. The effectiveness of current grid security standards are simulated when faced with actual attack scenarios as well as possible future attacks that become increasingly more sophisticated and threatening in nature. The simulations indicate that security upgrades involving improved lighting and visibility are not effective, while improved barriers are effective. More broadly, the limited effectiveness

of the proposed security upgrades suggests that there is substantial scope for research and testing, and for consideration of how utilities are securing electric infrastructure assets.

Chapter 5 considers critical infrastructure as a whole, evaluating federal emergency response and management across the different critical infrastructure sectors. Here, the goal is to determine how electricity sector response compares to the policy responses to the challenges and events impacting other sectors. Analysis across multiple large incidents affecting different components of critical infrastructure shows a largely linear and consistent relationship between the impact of a disaster in terms of both human health and cost, and the sum of the public sector funding and insurance response.

Attacks on the U.S. electric grid are a continuing challenge, as demonstrated in Chapter 2. In line with the prevailing risk perception literature, the analysis in Chapter 3 indicates that malicious attacks on the electric grid receive a larger response, in terms of federal R&D funding, than natural disasters or failures. This study finds that threats to national security are a driver of policy priorities and actions to both repair and improve the electric grid. Federal and state governments as well as the utilities and private sector bear significant costs when attacks occur. As concluded in Chapter 4, utility efforts to increase security are not fully public, but those that can be evaluated have significant weaknesses. Across all infrastructures, Chapter 5 demonstrates that government and private insurance payments largely pay fully for the impact of each disaster, irrespective of cause or sector, with terrorist attacks receiving emergency response funding at the same level as accidents and natural disasters. Similarly, federal research and development funding related to grid security has remained largely steady, with increases in response to large incidents irrespective of cause.

CHAPTER 1. INTRODUCTION

The electricity infrastructure sector in the United States is essential for the functionality of all other major critical infrastructure sectors. The infrastructure has been built over many decades by many different organizations and with different technologies; it extends to the remotest locations and also runs through areas that are highly accessible and public. As essential as the electricity infrastructure is to the U.S., it also remains vulnerable and the target of intentional malicious attacks. The overarching question examined in the following dissertation is: what are the threats that are impacting the electricity infrastructure in the U.S. and how are policymakers responding?

Centering around this question, the four chapters of this dissertation provide a retrospective analysis of targeted attacks on the gird, and then examine both present and future threats that can impact not only grid security, but also resiliency and reliability. Using this approach, valuable information is learned from past attacks and will ultimately help mitigate damages from future, and potentially more sophisticated, attacks. The questions of focus include: Is the vulnerability of electricity infrastructure a valid threat? If yes, have policymakers reacted, in terms of federal research and development funding, to improve electricity resiliency, reliability, and security? Specifically of interest is whether policymakers consider malicious to the electric grid as a more pressing issue in need of funding compared to naturally occurring weather events or other technical or human-caused failures.

A modeling analysis is then included to simulate mitigation strategies to protect grid infrastructure from both established methods of attack as well as potential future attack methods. From here, this dissertation research then looks more broadly across critical infrastructure sectors to examine the response to significant events that impact the electrical grid compared to significant events that impact other sectors. The research presented ultimately provides a robust understanding of the current threats to electrical infrastructure and whether the vulnerabilities are or are not adequately being addressed at the federal level.

1.1 Targeted Attacks Against U.S. Electricity Infrastructure

The dissertation research presented here begins with Chapter 2: a retrospective evaluation of intentional attacks on the electrical infrastructure sector in the U.S. from 1970 to 2016, with the purpose of assessing the overall threat to the sector. Threats against critical infrastructure are a function of vulnerability of the infrastructure, capability of the attacker(s), and the motivation behind the attacks (Kosal, 2006). Evaluating past attacks helps create a better understanding of what parts of the electricity infrastructure sector are most vulnerable and targeted, what methods of attack have been used in the past and how successful have they been, and what motivates assailants to target the grid.

Targeting critical infrastructure in an attack is not a new concept. Previous research in the terrorism and political violence fields indicate that attacks against critical infrastructure are intended to cause societal, political, and economic panic and disruption, as well as a breakdown in communication and information sharing (Devost et al., 1997; National Research Council of the National Academies, 2012). In more recent years, with

the increased accessibility of both the internet and computer programming, the potential threat of cyberattacks against critical infrastructure has grown. Studies of other sectors have indicated that cyberattacks are more appealing, allowing for less organization and smaller group size than physical attacks of the past (Holt, 2012).

While history is not predictive, information about past attacks and attack trends can be helpful when assessing the current and potential future threats to the grid. In Chapter 2, a novel database of physical attacks on U.S. electricity infrastructure is provided. All incidents recorded in the database required at least two sources (peer reviewed articles or books, reputable media sources, government reports) in order to be considered credible attacks and thus included. Details from the sources allow for an in-depth case study analysis of past attacks, where trends and changes over the past nearly 50 years are studied. In total, there were 52 intentional, malicious attacks on the U.S. grid between 2000 and 2016.

In evaluating these 52 attacks, the trends identified as most pertinent to this dissertation were the targets of attack, the methods used, the attacker profiles, and the motivation for attack. Determining the targets most often attacked helps pinpoint what kinds of infrastructure within the electricity sector are most vulnerable to physical attacks. Has the infrastructure targeted changed in recent years? Similarly, have attack methods changed between 1970 and the modern times, and is there a preferred weapon or style of attack when it comes to the electricity sector? Attacker profiles and attacker motivation, coupled together, assists in understanding what groups or individuals target electricity infrastructure and why. Here, motivational factors are divided into seven groups: protest to a single focusing event; disruption of government, economy, or the

operating utility; vandalism; theft; environmental activism; protests against U.S. foreign and military policy; and sabotage.

The results of Chapter 2 indicate that there is a long history of attacks on electricity infrastructure in the United States. The motivations for and characteristics of the attacks provides insight into ongoing risks to the electric grid. The data show a shift over the decades away from attackers communicating the motivation for their actions, to attacks that go unclaimed. This shift suggests that motivations change from protesting a specific event, policy, or government action to more general sabotage motivations. Malicious attacks with evidence of sophisticated methods or coordinated efforts are also noted, providing further insights into how threats are evolving. Despite the current twenty-first century focus on cybersecurity, physical attacks remain prevalent, therefore we recommend that states, utilities, and federal regulatory agencies recognize and mitigate physical vulnerabilities in addition to cybersecurity threats.

1.2 Federal R&D Funding Response to Incidents on the Electric Grid

While the Chapter 2 details who attacks the grid and why, the third chapter seeks to answer what, if anything, policymakers are doing to address the threat of intentional attacks on the grid. Electric grid infrastructure is vulnerable to resiliency, reliability, and security related issues due to a variety of factors. Disruptions on the grid are caused by severe weather events, technical and human-caused failures, as well as malicious attacks. The Energy Sector, which includes electricity infrastructure, is considered a national security issue, but do policymakers perceive a risk to national security when disruptions on the grid occur?

Risk perception is used as the theoretical foundation for evaluating this question. Previous studies focusing on risk perception have concluded that stakeholders are more inclined to address a given risk when they or someone they know are directly impacted (Leiserowitz and Smith, 2017). Similarly, an increased awareness and understanding of issues associated with a problem increases stakeholder's risk perception (Bostrom et al., 1994). Risks that are immoral or perceived as "unnatural" are associated with an increase in concern for a given threat (Sjoberg, 2000), as are events that are inherently known to be threats, such as war (Wildavsky and Dake, 1990). Based on the existing literature on risk perception, described in Chapter 3, it is expected then that policymakers will be more concerned (and therefore react) when the electric infrastructure is impacted by malicious attacks that illicit a threat to national security, rather than severe weather or human and technical failures.

To measure policymaker's concern and reaction to disruptions on the grid, fiscal year research and development (R&D) allocations from the Department of Energy (DOE) is utilized. Research on federal R&D funding indicates that higher fiscal year funding allocations are associated with more innovations and technological answers to emerging issues in the field (Kittner et al., 2017; Margolis and Kammen, 1999; Nemet and Kammen, 2007; Sterlacchini, 2012). Energy-related R&D has been decreasing while the total federal R&D budget has been increasing (Kittner et al., 2017), causing concern that this underinvestment will negatively affect the United States' ability to address emerging problems in the evolving energy landscape (Margolis and Kammen, 1999). Recent program evaluation research as shown that federal investment's in DOE R&D programs, such as the Advanced Research Projects Agency – Energy (ARPA-E) leads to both

technological answers to emerging questions as well as contributions to basic scientific fields (Goldstein and Narayanamurti, 2018). As the majority of grid-related R&D funding is allocated through the DOE's Office of Electricity Delivery and Energy Reliability (OE), the analysis uses the percent of fiscal year funding from the OE subset of budget data out of total DOE funding from the years 2003 to 2018.

Data for disruptions on the grid comes directly from utility owners and operators who report them to a joint Department of Energy-Department of Homeland Security database referred to as the OE-417 database (Office of Electricity Delivery & Energy Reliability, 2018a). This database includes disturbances on the grid that are considered "unusual" either in terms of load lost, duration of the outage, number of customers impacted, the kind of failure that caused a disruption, and suspected or confirmed physical and cyberattacks. Merging data collected from the years 2000 to 2017, there were 2,203 total reported disturbances on the grid, with 1,093 being related to severe weather, 582 being caused by human or technical errors, and 527 being suspected or confirmed malicious incidents.

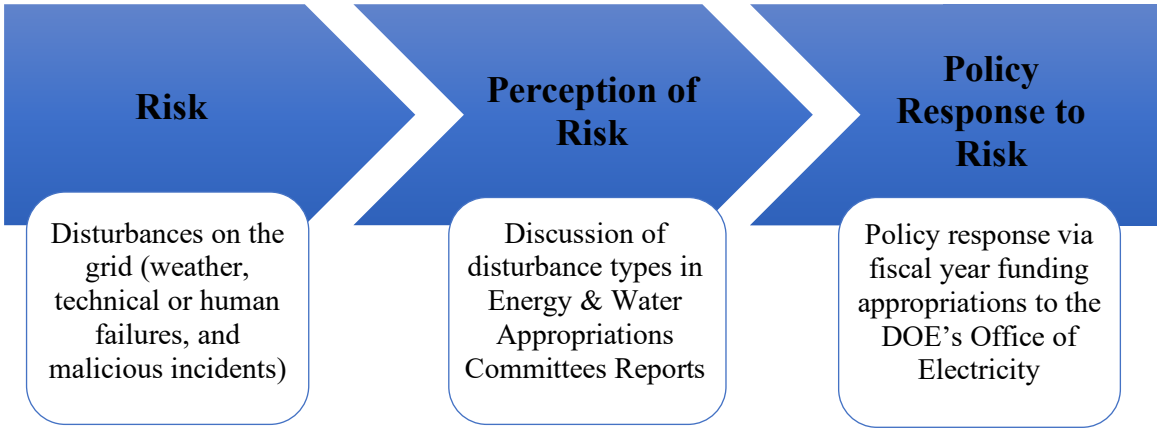

Figure 1-1. Risk Perception Process

Following the risk perception process in the supporting theoretical literature, stakeholder's perception of risk first depends upon communication and understanding of the given risk (Atman et al., 1994; Bostrom et al., 1994), though it is possible for stakeholders to consider something a risk because the risk is inherently known to be a threat (such as war or threats to national security), regardless of knowledge about the threat (Wildavsky and Dake, 1990). To measure this, Energy and Water Appropriations Committee Reports are analyzed for both the House and the Senate from 2003 to 2018. Utilizing text mining methods with in the documents, these reports provide an indicator of policy priorities in reference to disturbances on the grid relating to malicious attacks, severe weather events, and human or technical failures. The measure of policy response is then to indicated by an analysis of appropriation funding each fiscal year to the Office of Electricity. This process of risks, indicators or risk perception, and measured policy response are outlined in Figure 1-1.

A time series regression analysis is utilized to assess whether an increase in malicious attacks on the grid is are perceived as a threat, therefore resulting in policymakers allocating more federal funding for grid-related R&D. Due to the inevitable delay between when incidents occur and when policymakers enact funding, a Finite Disturbed Lag model is used to evaluate DOE and Office of Electricity budget allocations one, two, and three years after the year the disturbances took place. (For example, with a three-year time lag, disturbances that occurred in the year 2000 would not influence funding allocation decisions until the year 2003). The time series regression analysis also seeks to determine if media attention on the disruptive events and the political party in control of the House, Senate, and Presidency is associated with policymakers allocating

more R&D funding in a fiscal year. Conversely, I also test to see if the number of incidents or cause of incidents do not matter, and rather an increase in the magnitude of the disturbance (total number of disturbances each year, duration of the outage, amount of load lost, number of customers impacted) is associated with an increase in fiscal year funding.

The results of the analysis conclude that policymakers respond to malicious disturbances on the grid in the first year after the event. The response is in line with an increase in congressional discussion of malicious risks in the Appropriation Committee Reports. The results provide a novel approach to risk perception and policy response, as well as indicate a preference among congressional policymakers to fund preventative measures to threats to national security more so than regularly (and naturally) occurring severe weather events.

1.3 Will Updated Electricity Infrastructure Security Protect the Grid?

Using the detailed information collected on past physical attacks from 1970 to present day in Chapter 2, Chapter 4 provides an assessment of the vulnerability to attack of the U.S. electric grid today. While Chapter 3 seeks to determine how federal policymakers address grid security concerns, this chapter uses existing security standard information from private utilities and the regulating authority North American Electricity Reliability Corporation (NERC). The overarching question addressed is whether proposed and implemented security standard upgrades for grid infrastructure are adequate in mitigating damages from attacks as well as preventing future attacks.

To address this question, a series of models is were built using the Joint Conflict and Tactical Simulation (JCATS) software program, which is developed by Lawrence

Livermore National Laboratory (LLNL) and primarily used to simulate wargame outcomes using user-defined data (Lawrence Livermore National Laboratory, 2017). Here, the user-defined data are the details of the actual physical attacks that occurred on the grid identified in Chapter 2. Additional data collected and entered into the JCATS model includes the current and proposed security standards for grid infrastructure, collected from utilities, NERC, and government reports (National Research Council of the National Academies, 2012; North American Electricity Reliability Corporation, 2015a; Pacific Gas and Electric, 2014). Security improvement standards include reducing foliage around a site and increasing lighting, increasing the number of security guards on site, adding cameras and sensors, and improving perimeter fencing and internal walls and shielding.

In the JCATS model, feasible physical and cyber-enabled physical attacks are modeled against the current and proposed security standards for a U.S.-based generic electric substation. Next, a series of increasingly sophisticated physical attacks are simulated on the substation, as are a set of cyber-enabled physical attacks. Again, using detailed data from Chapter 1, three levels of attacker profiles are created to indicate the increasing ability and training levels of attackers. Attackers primarily use firearms in the attack scenarios, though the most sophisticated attackers also use improvised explosive devices. Necessary data that was provided either within the JCATS program itself or from critical infrastructure and military experts at LLNL include the probability of attacks to acquire and successfully strike the targets (transformers) within the substation during an attack.

The findings indicate that some of the updated security measure are effective at mitigating damages to electrical infrastructure, while some are not. Specifically, additional barriers around the substation and physical armored protection of transformers reduce the amount of damage inflicted from both physical and cyber-physical attacks. In contract, additional cameras, sensors, and reduction in foliage are not as effective. This case study demonstrates an approach to testing the efficacy of physical security measures that can assist in decision-making for critical infrastructure security.

1.4 Public and Private Response to Incidents Impacting Critical Infrastructure

The final chapter of my dissertation compares the response (or lack thereof) to major disasters in the energy infrastructure sector to the response to other disasters across critical infrastructure sectors. As defined by the Department of Homeland Security, there are sixteen critical infrastructure sectors in the United States and disasters included in the event database that I have developed include natural disasters, accidents, illnesses, malicious events, and general system failures. This chapter seeks to determine whether there is a relationship between the size of the disaster's impact and the federal or state response.

The magnitude of the disasters included in this analysis are evaluated based on the impact the disaster had on society, in terms of human health impact and monetary cost impact. The impact is then compared with public sector response to the disaster, as well as to the subsequent insured losses. Public sector responses are broken into two categories: Federal Emergency Management Agency (FEMA) response and all other assistance provided by federal or state agencies or governments. Human health impact is monetized using commonly used methods in order to be compared with federal and state

monetary responses as well as the private sector response (insured losses) for each event. Included in the dataset are a wide range of disasters, with each one assigned to the main critical infrastructure sector that the event impacted. The relations between impact and policy response are compared as power-law relationships in order to examine response patterns over events of widely ranging scales.

The results of this analysis indicate that the public sector response roughly proportionally to the human health impact of a disaster, as does the private sector. Furthermore, the results suggest that there may be some sectors, such as the Chemical and Food and Agriculture sector, where a privatization of the industries within it result a larger monetary private response than public response after disasters. Public response maybe instead be in the form of policy regulations, rather than monetary funding.

CHAPTER 2. TARGETED ATTACKS AGAINST U.S. ELECTRICITY INFRASTRUCTURE

"Conventional threats are always evolving, which makes protecting the grid as it is today very difficult. Just think about it, a person can now buy ten self-flying drones off ebay, load them up with explosives and have them dive bomb on to critical power nodes. Such a threat didn't exist five years ago."

-Jon Wellinghoff, Former Commissioner of the Federal Energy Regulatory Commission (Register, 2015)

2.1 Introduction

The security of critical infrastructure in the United States has long been an underlying issue (Post et al., 2000). In the years following the September 11 terrorist attacks in 2001, a new sense of urgency has brought focus on the U.S. critical infrastructure, including the electricity infrastructure grid (National Research Council of the National Academies, 2012). In October of 2002, Osama bin Laden called for Al Qaeda to "target key sectors of the U.S. economy" in future attacks, with sectors including transportation, telecommunication, financial institutions, agriculture, water supply, the chemical industry, and, of course, energy-related infrastructure (National Research Council of the National Academies, 2012). The concern is justified, seeing as energy and the electricity infrastructure (commonly referred to as the electric grid) in the United States has repeatedly been a target for attacks for nearly 50 years, albeit attacks on a relatively small scale. These past attacks indicate not only that the nation's electricity infrastructure is vulnerable, but also that it is a known weak point for attackers to target with relative ease. Electricity infrastructure in the U.S. is vast, including power plants, transmission towers, low- and high-voltage transmission lines, distribution substations,

and natural gas pipelines to power plants and utilities. Furthermore, the infrastructure spans great distances across the country, resulting in key, and sometimes the quite vulnerable, infrastructure being isolated and insecure in remote locations.

A 2014 study by the Federal Energy Regulatory Commission (FERC) on the nation's electricity system stated that a coordinated attack on "just nine of the country's 55,000 electric-transmission substations" during peak electricity demand could cause cascading blackouts across the country (Smith, 2014a). The FERC report highlights the slow response to secure electricity infrastructure over the past decade and a half. Despite the initial call for improved security across key sectors immediately after September 11, key industries and infrastructure were still vulnerable in 2004, prompting renewed concern from the Department of Homeland Security (DHS) following the Madrid bombings, and security has continued to be a priority for electricity infrastructure in particular, even after multiple reports have emphasized the need for critical infrastructure (including electricity infrastructure) security improvements, and as seen through various Congressional bills that have been proposed in recent years (Cantwell, 2015; Markey, 2010; Murkowski, 2015; National Research Council of the National Academies, 2012; Public Health and Welfare, 2001; Sarbanes, 2015).

Electricity infrastructure attack are not restricted to the United States. Terrorists have targeted natural gas pipelines, electrical grids, power plants, and other related infrastructure across the world, including in Colombia, Peru, Thailand, Iraq, Pakistan, the United Kingdom, and in Africa (Giroux et al., 2013; National Research Council of the National Academies, 2012). Power generation stations have been attacked in Baghdad in recent years, while the Irish Republican Army bombed electricity infrastructure in the

United Kingdom in the 1990s (Montalbano, 1996; National Research Council of the National Academies, 2012). Attacks on energy infrastructure in general (which includes both on and offshore oil and gas production sites, storage facilities, and coal mines) has been increasing worldwide since 2001, particularly in Colombia, Iraq, and Pakistan (Giroux et al., 2013).

The combination of electricity infrastructure being a known target, the remoteness of infrastructure, and the looming threat of a large-scale attack has prompted an increase in assessments, reports, and provisions to address inadequate security. However, these efforts are aimed at addressing *vulnerability*. While vulnerability is certainly a key concern and an aspect where improvements can be seen and measured, it is just one factor in the overall *threat* of electricity infrastructure attacks.

Following Kosal's 2006 study on Terrorism Targeting Chemical Facilities, the threat of an attack is a function of vulnerability of the infrastructure, capability of the attacker, and the motivation behind such an attack (Kosal, 2006). While the vulnerability of U.S. electricity infrastructure is clear (and will be described briefly in the next section of the paper), the capability of would-be attackers to carry out a successful and large-scale attack is subject to debate amongst utility and industry experts, and thus will not be addressed here. Therefore, the main focus is to explore the motivational factors behind electricity infrastructure attacks in the United States. By focusing on motivations for attacks over the past few decades, a more complete understanding for how and why energy infrastructure is attacked can be gained and how unsophisticated attacks may provide insight for future sophisticated attacks. This will ultimately add to the overall

evaluation and understanding of the threat to electricity infrastructure and provide insight and guidance into future federal and state security standards and policies.

The following section will first outline the critical role energy and electricity infrastructure plays in the U.S., as well as some of the fears associated with a possible attack to this sector. The second section describes the reports and policy efforts that have attempted to highlight the vulnerabilities of the grid and sometimes propose solutions. A literature review follows, highlighting previous research on terrorism and critical infrastructure security, particularly paying attention to existing databases that either touch upon or are directly concerning critical infrastructure attacks. Next, the data sources and methodologies used in creating an incident database are described, including categorization of attacks on U.S. electrical infrastructure with key parameters, such as date, location, attack target, attack method, and attacker motivation. We then explain in more detail the motivation behind the incidents, which provides valuable information in the next section for assessing how, where, and through what methods and outside factors has the electricity infrastructure been targeted and the frequency of such incidents. Lastly, we discuss the key implication of the study's results and the emergence of sophisticated and coordinated attacks, followed by conclusions and recommendations.

2.2 Critical Infrastructure as a Target

Targeting critical infrastructure in order to disrupt the economy, society, or the current political arena is not a new concept. In his 1997 article, Devost and his co-authors discuss the concept of "information warfare," meaning the purposeful attack against critical infrastructure that supports communication methods or the infrastructure that relies upon the distribution of information to function (Devost et al., 1997). The goal of

attacks of this nature is to cause panic, disruption, and potential breakdowns in the infrastructure that keeps society and the economy functioning safely and reliably. Furthermore, the ever increasing threat of cyberattacks poses a particular threat for infrastructure, such as electricity infrastructure, that is reliant upon cross communication throughout the system, and cyberattacks can lead to physical disruptions and destruction. As technology modernizes, so too do the methods attackers may choose to use. Attackers that used to physically cause disruption in order to convey a political or social message may now be more inclined to switch to being disruptive through cyberattacks (Holt, 2012). While a physical attack, such attempting to topple transmission towers, might require a small group of actors, a cyberattack could easily just be a single actor. With the prevalence of information available online, the know-how needed to successfully conduct an attack is greatly reduced, thus increasing the possibility and dangers of lone wolf attacks (Ellis, 2014) in both the physical and cyber realms.

2.3 Vulnerability of the Electrical Infrastructure

The electricity infrastructure is one of the nation's key critical infrastructures. All other critical infrastructures in the U.S. depend on the electricity industry, including energy production services, emergency and health services, financial services, and communication services. Both the former chief of the Central Intelligence Agency (CIA), Jim Woolsey, and former Commissioner of the Federal Energy Regulatory Commission (FERC), Jon Wellinghoff, have emphasized that the nation's electric grid is a known and vulnerable target for terrorists, and a sophisticated attack could handicap the electrical supply for much of the nation (Register, 2015).

The vulnerability of the electricity sector can be attributed to a number of factors, though only a few will be discussed here. First is that the use of electricity infrastructure today is quite different from how the system was originally designed. While power systems were designed to service individual regions through a vertically integrated utility model, calls for an increase in market competition led to the restructuring of the electrical distribution system in some parts of the country. Power system structures can supply distant neighbors, leaving many power stations and transformers (systems installed at key points on the grid where voltage must be transformed from high to low, or vice versa) stressed with the distribution of power through high-voltage transmission lines (Electricity Forum, 2015; National Research Council of the National Academies, 2012, p. 2).

Second, and to complicate matters more, electricity generation and transmission is owned and managed by a combination of private investors, public (state and federal level), and independent operators. Therefore, not only are much of the security options left up to the various operators, but also that one utility's insecure infrastructure can lead to outages in another state. An example of such an event was in 2011 when a transmission line at a substation in Arizona failed, resulting in massive outages in San Diego, California, as well as into Baja California, Mexico, causing millions of homes to be without power for the better part of a day (Watson, 2012). Similarly, but on a larger scale, the 2003 Northeast blackout caused more than 50 million people to lose power, some for multiple days, spanning from Michigan to Massachusetts, as well as into mid and northeast Canada. The cascading blackout across independent service operators was caused by a combination of technical failures, human failures, and weather-related incidents (U.S.-Canada Power System Outage Task Force, 2004a). The blackout

ultimately cost $4-6 billion, or approximately $5 for every forgone kilowatt-hour generated (at the time, electricity cost $0.093 per kilowatt-hour)(National Research Council of the National Academies, 2012, p. 16).

Weather and technical failures aren't the only non-human event that can cause damages and outages to electricity infrastructure. Squirrels have caused more power disruptions than physical and cyberattacks combined in the U.S., with 137 squirrel-related outages in 2015 alone ("Cyber Squirrel 1," n.d.; Dews, 2014; Ingraham, 2016). Though it is not possible to prevent squirrels from climbing on the vast amount (and often remote) electricity infrastructure in the U.S., it is still important to learn from these disruptions. If a squirrel can inadvertently down power lines, cause monetary damages, and disrupt the power supply, why wouldn't an intentional attack be able to do the same, if not more?

Another critical but weak point in electricity infrastructure on the grid are transformers, (systems that convert high- to low-voltage or vice versa). Transformers are vital in keeping energy flowing from power generating plants into cities and also across large geographic areas, however, they are also expensive and time consuming to construct. Many of the components and materials are only available from a few suppliers, some of which are internationally located (Office of Electricity Delivery & Energy Reliability, 2012, p. 12). This means that not only are there only a few spares readily available, but also there would be a delay in manufacturing and constructing a new transformer in the event of an attack or failure of a transformer (Salmeron et al., 2004).

Last, one of the most focused upon weaknesses of the electricity infrastructure is that it is remote, aging, and not regularly maintained and updated to keep up with

technological advancements (Massoud, 2003; National Research Council of the National Academies, 2012, p. 2; Register, 2015). Aging electricity infrastructure allows for power outages to occur more often due to both weather related incidents and technical failures (Office of Electricity Delivery & Energy Reliability, 2012, p. v). Furthermore, the span of energy infrastructure is vast, with transmission lines and pylons snaking through mountain ranges, and transformer and substations left relatively unsecure in remote locations. The combination of the infrastructure's age and rural situation leaves the systems vulnerable to not only technical failures and weather incidents but also targeted attacks. The attack on a single transmission line can cause a cascading effect, severing power from nearby lines. Transformers in substations are key to sending electricity across large portions of the grid, therefore the loss of one transmission station could lead to outages and stressed power supplies in neighboring regions, as well as long repair delays as described above (Office of Electricity Delivery & Energy Reliability, 2012).

2.4 Databases and Research on Critical Infrastructure Attacks

Before we discuss our analysis, we explore previous research that has also created databases of attacks or incidents against critical infrastructure, paying particular attention to electricity infrastructure. The studies and databases described below provided helpful information and starting guides as we created our database, however none provided a complete and comprehensive list of attacks against U.S.-based electricity infrastructure, which is our ultimate goal.

There have been a few different research projects focusing on modeling infrastructure reliability and resiliency, as well as methodologically calculating the most vulnerable and critical infrastructure (Apostolakis and Lemon, 2005; Salmeron et al.,

2004). Salmeron et al. in 2004 tested various terrorist attack scenarios in a mathematical model in order to try to identify where the most critical components of the electricity infrastructure was located and offer suggestions for improving the reliability of the systems against future attacks (Salmeron et al., 2004). The researchers found that the U.S. electricity infrastructure is weakened technologically as electricity demand increases across the country. Furthermore, transformers were identified as a weak point for the sector, and Salmeron et al. suggest that "generic" transformer spares be manufactured and strategically placed across the country. Though the generic systems would not be a perfect match for all of the substations, they would at least allow for power to remain sufficiently flowing until the exact model of transformer needed was constructed and delivered (Salmeron et al., 2004).

Similarly, other literature models specific scenarios or incidents at the various energy infrastructures that may result in disruptions or breakdowns. Brown et al. create a program to model the vulnerabilities at the U.S. Strategic Petroleum Reserve, as well as on the electric grid in general (Brown et al., 2006). Boin et al. study the response and preparedness of catastrophic breakdowns in critical infrastructure using Hurricane Katrina as an example while Kashubskey investigates attacks targeting on and offshore oil and gas infrastructure worldwide from 1975 to 2010 (Boin and McConnell, 2007; Kashubsky, 2011).

Other past research has focused on attack motivations, such as the 2007 Ackerman et al. study funded in part by the U.S. DHS, and Giroux et al.'s 2013 Energy Infrastructure Attack Database (Ackerman et al., 2007; Giroux et al., 2013). The Energy Infrastructure Attack Database tracks attacks against energy infrastructure specifically

(including on and offshore oil and gas infrastructure, biomass, geothermal, wind, and solar infrastructure, and other fossil fuel sites, such as coal), dating back to 1980. Though the database includes at least 50 countries, it is unclear why some, such as the United States, are excluded. Regardless, the database offers many insights to energy-specific attacks across the globe. For example, attacks have increased at least 50% from 2001 to 2011 compared to pre-1999 levels, with an average of 400 attacks per year worldwide. Attacks tend to be focused on oil and gas infrastructure most often, and the researchers associated with this database also found evidence that investment and construction contracts for energy infrastructure tend to decrease if a region has experienced an attack against that sector. Bombs are the most popular method of attack worldwide, and Colombia, Pakistan, and Iraq are the countries with the most attacks per year, on average (Giroux et al., 2013).

Loadenthal's 2014 study provides insight into eco-terrorism attacks, where he asserts that the attacker's "soft targets," such as attacks against property, should not be considered acts of terrorism because they do not lead to death or injury. Loadenthal's database includes attacks against cars, trees, farms, businesses, and even McDonalds, located across North America and the U.K. Though Loadenthal's choice of perpetrator (the eco-terrorists) may not be intending large-scale harm or damages, his reasoning goes against well-established concern about the extent of damage that can be caused by property attacks alone, especially when it comes to electricity infrastructure (Post et al., 2000; Register, 2015; Sovacool and Brown, 2010).

2.5 Data & Methodology

For this analysis, the database of attacks on energy and electricity infrastructure in the United States was created in order to study the phenomena and consequences. An initial starting guide for our database comes from unusual disturbance reports, gathered by the U.S. Department of Energy (DOE) and in collaboration with the Department of Homeland Security (DHS). These reports are consolidated into a database, referred to as Electric Disturbance Events (OE-417), and include not only targeted attacks, but also weather- and technical-related disturbances impacting U.S. electricity infrastructure from 2000 to 2016 (Office of Electricity Delivery & Energy Reliability, 2018a). Utility operators, reliability coordinators, and balancing authorities are required to report incidents to the DOE if any of the following criteria are met: suspected physical or cyberattacks, interruptions due to a physical attack, interruptions due to a cyberattack, operational failure or shut-down of transmission or distribution, islanding during a blackout, an uncontrolled loss of at least 300 megawatts for 15 minutes or more, emergency load shedding of at least 100 megawatts, voltage reduction of at least three percent, or a public request to reduce electricity on the system (Office of Electricity Delivery & Energy Reliability, 2018a). In-depth records of incidents and disturbances on the U.S. grid unfortunately are not available from the DOE OE-417 reports, a limitation for the dataset to be explained further below, nor do the reports begin before the year 2000. However, we utilized other reports and data collection methods to include as many incidents as possible from 1970 to 2000, as well as any incidents the DOE may have missed from 2000 onwards.

Particularly helpful in providing information about incidents that happened in the 1970s and 1980s is the Terrorism and Response to Terrorism (START)/Global Terrorism Database (GTD). The START/GTD database an extensive system that catalogs terrorist attacks worldwide and for a variety of targets and motivations, including eco-terrorism and other politically motivated attacks, attacks against oil and gas infrastructure, nuclear facilities, and other energy sectors (Global Terrorism Database, 2015). The University of Maryland maintains the system and was a helpful guide in the initial planning stages of this analysis, as will be described in more detail in the following section. However, this database is not necessarily complete, with many incidents that are reported by major newspapers (New York Times, for example) going unreported in the START/GTD database.

The University of Maryland's START/GTD was used as a guide for our data categorization process (specifically for attacker motivation) and to identify key utilities that have been targeted multiple times, as well as reoccurring organizations or individuals involved in such attacks (Global Terrorism Database, 2015). Some incidents reported in the START/GTD do not have citations or the original citations can no longer be located. Thus, observations included in the database are included only if the following criteria is met: the incident is reported by the DOE or if there are at least two sources available describing the incident. Data were gathered through the OE-417 reports, published newspaper and media reports, books, journal articles, and industry or government reports.

The preferred method of gathering data for our database (outside of the OE-417 reports) was through Internet searches and searches via the LexisNexis Academic portal. Incidents included in the database are either directly from the OE-417 reports, from

books and journals dedicated to investigating critical infrastructure or terrorist attacks, statements in industry or government reports, or verbatim reporting in newspaper and media reports. Unofficial sources, such as blogs, Wikipedia, or online community postings were excluded. Ultimately, observations in the database include attacks on electricity infrastructure, such as power plants, electricity and grid-related structures and systems, and natural gas pipelines supplying utilities and power plants. However, cyberattacks, attacks on natural gas storage facilities, and attacks on nuclear facilities are excluded, for reasons explained below.

2.5.1 Exclusions:

Select OE-417 Data: A limiting factor in the accuracy of the OE-417 report database is that the reporting requirements are vague and therefore open to interpretation. For physical attacks, the OE-417 form asks utility operators to report whether a "physical attack," "suspected physical attack" or "suspicious activity" occurred. Utilities can then subcategorize the attack into theft, suspected or confirmed sabotage, suspected or confirmed vandalism, or unknown. While the reporting of an incident makes it clear that some type of unusual incident occurred on utility property, the distinction between vandalism and sabotage is not clear (especially when the incident might just be "suspected"). In short, the database cannot reliably assure that similar incidents are categorized consistently across locations (vandalism at one location could potentially be considered suspected sabotage at another location). Due to this uncertainty, we exclude OE-417 reported data from our analysis of attacker method and motivation, with the exception of reported incidents also in the media and reported theft. Incidents of theft are

more clearly defined in the reporting requirements and are of particular interest to utilities during periods of high copper prices. The remaining incidents analyzed for method and motivation have been reported on outside of the OE-417 database by multiple sources that includes media, industry reports and publications, and peer reviewed journals and books.

Cyberattacks: Although the susceptibility for physical electricity infrastructure and the technology used at power plants and for electricity transmission are both associated with age, cyberattacks and incidents of hacking are excluded from this database, as mentioned previously. This is in part due to the lack of concrete reporting on such attacks that include specific information necessary for the database, such as dates, locations, attack origin, and motivation. Publicly available records of cyberattacks are very limited, partially because many attacks go unnoticed, but also because the attacks may be classified (Burke and Fahey, 2014). While the DOE OE-417 reports do include suspected and physical cyberattacks, the usefulness of these reported incidents gets overshadowed by the amount of recorded suspected or confirmed physical attacks. It is also excluded because the technology associated with system operations is not targeted through physical attacks and therefore not subject to the same vulnerabilities of rural and expansive infrastructure. Lastly, cyberattacks are excluded because the threat of a widespread and/or long-lasting blackout due to a cyberattack alone is not as severe as with a coordinated attack on physical electricity infrastructure (National Research Council of the National Academies, 2012).

Nuclear and Oil & Gas: The nuclear energy and oil and gas industry have different security concerns compared to other electricity infrastructure, such as natural gas pipelines and electricity generating and transmission infrastructure, and therefore also excluded from the dataset. Due to the immediate catastrophic consequences of a nuclear meltdown, the Nuclear Regulatory Commission regularly updates security standards and guidelines and conducts Force-on-Force security exercises (multi-day mock-attacks and field simulations) every three years at nuclear facilities (U.S. NRC, 2015). Threats to oil production and large natural gas and liquid natural gas storage facilities are also excluded. An exception to the exclusion is if the attack is aimed at electricity infrastructure outside such a facility but directly related to powering the facility, such as transmission lines.

2.6 Motives and Intent for Attacks

The final database analyzed here details 52 incidents total from 1970-2016. Of the total attacks between 2000 and 2016, 16 are recorded both by media reporting and the DOE OE-417 database. The remaining 36 incidents we include in our database occurred between 1970 and 1999 and are detailed through media accounts. The attacks occur in 42 states, plus in Washington D.C. and Puerto Rico. Each incident is categorized by date, location, name of targeted infrastructure, attack method, and motivation.

Also included are descriptions of the infrastructure targeted in the attack, such as power or transmission lines, power stations or substations, utility poles or pylons, transformers, pipelines supplying natural gas to utilities and power generating plants, and company offices. Most pertinent to this analysis is the categorization of both methods and motives of the attack. The attack method is categorized as either an explosive device,

firearms, arson, suspicious activity, theft, and physical sabotage or destruction. The principal motive or intent of the attack is grouped as one of the seven following: 1) an attack in protest or reaction to a focusing event; 2) an attack aimed at disrupting the government (federal or state/territory), economy (federal or state/territory), or utility company; 3) an attack aimed at condemning the target for an environmental-related reasons (such as pollution or energy inefficient practices); 4) an attack in protest or reaction to U.S. foreign policy, including military action; 5) an attack that is known to be vandalism; 6) an incident of theft from the site; and 7) an attack that is sabotage of the infrastructure where any primary motive other than to cause physical destruction is unable to be specified.

When applicable, the attacker motive is further categorized into the following groups: motivated by political ideology, motivated by religious ideology, motivated by separatist intent, or indicates an attack, or series of attacks, appear to be sophisticated and/or coordinated. Political ideology breaks down further into the following subgroups: eco-terror, sovereign ideals, Communists, and other indistinct left wing or right wing groups. Motives and intents will be described in further detail in the following section.

The motivations and intent for electricity infrastructure attacks in the U.S. is broken down into seven key categories: an attack in protest or reaction to a focusing event; an attack aimed at disrupting the government, economy, or utility company; an attack motivated by environmental-factors; an attack in protest or reaction to U.S. foreign policy, including military actions; an attack that is an act of vandalism; an incident of theft; and an attack of physical sabotage. The categories are not discrete, however, and some observations in the dataset are noted to have more than one motive.

2.6.1 Attacks in Protest or Reaction to a Single Focusing Event

A primary motivator is a single focusing event that ignites a group or an individual to demonstrate their dismay through protests, which can be in the form of a targeted attack. Attacks of this nature occur 16 times in our dataset, all before the year 2000. Attacks stemming from focusing events are nearly all in the honor of a deceased individual whose death, attackers believe, was unwarranted (The one exception is an attack in December of 1999 where the focusing event was attributed to Y2K-related terrorism)(Gladstone, 2015). Attackers often have created an organization in the name of the deceased and adopt a few fundamental beliefs or an ideology to center around. This behavior is seen with Grupo Estrella in Puerto Rico the early 1980s and the Georgia Jackson Brigade in the Pacific Northwest the late 1970s. When a focusing event relevant to their cause would occur, the group would rally and stage attacks, calling in to radio stations or newspapers to communicate why they attacked or what they demanded.

Grupo Estrella was named after Saul Rodriguez Estrella, a Puerto Rico Electric Power Authority worker who died while participating in a strike against the Power Authority. While the local police claim that Estrella was killed while attempting to sabotage transmission lines, Grupo Estrella disagrees, and hence their namesake. Grupo Estrella attacked the Puerto Rican Electric Power Authority at least twice, once on April 18, 1980 and again on August 27, 1981, with the focal events being workers' rights. The 1980 attack on a Puerto Rican Electric Power Authority substation in San Juan was in protest of the Power Authority supposedly violating "the collective bargaining agreement" while negotiating new contracts with the workers (Wheaton, 1980). It is unclear exactly what occurred during the attack, but an engineer working for the Power

Authority was kidnapped and the resulting blackout left 3.3 million people without power (Counterterrorism Threat Assessment and Warning Unit Counterterrorism Division, 1999; Wheaton, 1980). In 1981, Grupo Estrella placed an explosive device at a power station, which caused hundreds to lose power. This attack was in solidarity with 6,000 Puerto Rican Electric Power Authority workers, who were currently on strike from the company and demanding higher wages (Counterterrorism Threat Assessment and Warning Unit Counterterrorism Division, 1999; Global Terrorism Database, 2015).

The George Jackson Brigade was a little less focused than Grupo Estrella; it generally had communist ideals and asserted it was fighting for prisoners' rights and equality amongst genders and races (Perry, 2015) (However, of the four incidents credited to the George Jackson Brigade in this dataset, only the following incident is categorized as a protest to a single invent. The other three attacks are categorized with the intent to disrupt the government, economy, or a utility company.). The group adopted their name after George Jackson, a Black Panther member, was killed trying to escape from San Quentin prison in 1971 (Perry, 2015). The first Brigade attack on electricity infrastructure was in Seattle, Washington on December 31, 1975. The group bombed the substation that powered a wealthy suburban neighborhood of Seattle in an act of solidarity with the City Light workers who were currently on strike. The workers on strike then refused to fix the substation (Burton-Rose, 2010; Hewitt, 2005).

2.6.2 Attacks Aimed at Disrupting Government, Economy, or Utility

Attacks against the local or federal government, economy, or utility company tend to be in the name of a general goal or cause, and these attacks occur indiscriminately regardless of a focusing event. The attacker(s) strike with the intent to disrupt society,

either by causing fear and anxiety or economic disruptions, or with the intent to disrupt government or utility operations. The attackers aim at eventually achieving a goal through the disorder they cause, hoping to incite the government, utility, or society to react in the way the attackers have planned. Below describes a handful of the 27 total attacks aimed at disrupting governments, utilities, or economies.

The Provisional Coordinating Committee of the Self-Defense Labor Group in Puerto Rico attacked both the Department of Natural Resources and a substation on April 30, 1982 in an attempt to force the government and utility to improve worker unions and labor conditions. In these coordinated attacks, 20,000 households lost power and a guard at the utility was taken hostage (Kushner, 2002; Pala, 2015). A quite different example is that of the November 2, 1983 attack by the right wing religious group, the Covenant, Sword, and Arm of the Lord. The group set off dynamite at a natural gas pipeline in Fulton, Arkansas, with the goal of cutting off energy supply to the region as the temperatures drop, thus starting societal unrest that the group believed would lead to a holy war (Hamm, 2007).

The remaining three attacks by the George Jackson Brigade (as described above) are also categorized as attempts to disrupt government or the economy. The Brigade was responsible for several dozen bombings and robberies in the late 1970s. The group was no longer being motivated by a single focusing event, such as a worker's strike, but instead intended to cause havoc to the local government, economy, and society through their attacks throughout the state of Washington. Police issued a ban on media reporting about the Brigade's attacks, for it was seen that the attackers mostly wanted attention. Despite this, the George Jackson Brigade bombed three different electrical infrastructure

locations between 1976 and 1977, though only two of the bombs went off successfully (Burton-Rose, 2010), (Perry, 2015), (Burton-Rose, 2010).

More recent attacks aimed at disrupting government, economies, or utilities occurred in in Texas, Arkansas, and Massachusetts. In 2012, a Texas man named Anson Chi used a homemade explosive device to try to blow up an Atmos Energy natural gas pipeline. Though the device did not rupture the pipeline, it did injure Chi, who declared that he acted as part of the sovereign citizen movement. Chi was sentenced to jail and to pay Atmos Energy $28,127 in damages (MacNab, 2012; Wigglesworth, 2015). Similar in anti-government sentiment were the series of attacks in Arkansas between August and October of 2013. Here, the perpetrator targeted power poles and pylons through physical destruction and sabotage, as well as setting fire to an extra-high voltage switching stations. An August attack, involving a train severing a 500,000-volt powerline the attacker had purposefully caused to fall onto the tracks, lead to damages estimated at $550,000 in damages. A September arson attack at the switching station caused an estimated $4 million in damages. Damages over $100,000 require federal investigation, with the FBI ultimately arresting Jason Woodring who lived nearby some of the powerlines he was sabotaging. Though a specific reason behind the attacks is unclear, Woodring gave anti-government statements to investigators and was ultimately sentenced to 15 years in prison (Carter, 2013; FBI, 2015).

A clear reason was given in the 2016 attacks against the National Grid power lines in Massachusetts. In this incident, the attacker strung multiple incendiary devices along powerlines, with one actually igniting, and left a note stating that the National Grid needed to help him change the U.S. court system and provide him with large monthly

payments, otherwise he would continue to place these devices on powerlines. The FBI traced the local-area man, Dan Kelly, where he was arrested and sentenced to five to twenty years in prison and ordered to pay a $250,000 fine (Rosen, 2016; Valencia, 2016).

2.6.3 Attacks Motivated by Environmental Factors

Environmentally motivated attacks are characterized by the assailant's dismay against an environmental-related activity conducted by either the government or a utility. The six environmental attacks in this database are all categorized as attackers with a set political ideology (self-identified as liberal) but subcategorized as eco-terrorist incidents. Eco-terrorism, referring to environmental terrorism (Alpas et al., 2011), has been categorized for usually attacking "soft" targets, meaning targets that are vulnerable, easy to access, or relatively isolated (Loadenthal, 2014). Eco-terrorist tend to take care to try to not harm the environment, animal wildlife, or humans in their attacks and tend to include acts of physical sabotage, destruction, graffiti, and arson (Loadenthal, 2014).

In the U.S., environmentally motivated attacks against electricity infrastructure were most common in the late 1980s, with environmental terrorist attacks targeted infrastructure relating to or supporting nuclear facilities. On May 14, 1986, supposed eco-terrorists threw metal weights onto high voltage power lines, causing them to short circuit, at the Arizona Nuclear Power Project. The facility was currently under construction, and the completion date had to be pushed back (Lopez, 1986). Similar attacks then occurred elsewhere in Arizona at two other nuclear facilities. First, on September 25, 1988, members of the Evan Mecham Eco-Terrorist International Conspiracy Group sawed down 34 utility poles powering Energy Fuels Nuclear uranium mines (Jarboe, 2002). This attack caused more than $1 million in damages and two of the

mines lost power. On May 30, 1989, the Evan Mecham Group attacked again, this time at a U.S. Department of Energy facility in Wenden, where the group was caught attempting to cut through metal support towers (Jarboe, 2002).

2.6.4 Attacks in Protest Against U.S. Foreign or Military Policy

Attacks motivated by U.S. foreign policy, including military decisions, are the third most common motivational factor included in this database. However, in a few of the incidents, an attack in protest to a single focusing event is the primary motivator, with protest against U.S. foreign policy being secondary. Motivation for attacks on critical infrastructure can be straightforward, such as in Puerto Rico, where the attacking group was a separatist organization. However, the intent for the attack can also be unclear or unknown until the perpetrator is caught or comes forward. Attacks of this nature have not yet been intended to cause widespread destruction or fatalities, but FERC has noted that this motivation for attack is of concern for the agency (National Research Council of the National Academies, 2012; Smith, 2014a).

As an example, in 1981 the separatist group Macheteros detonated pipe bombs at two Puerto Rican Electrical Power Authority stations in San Juan. Nearly 20,000 homes lost power, including luxury resort hotels on the beachfront, and the blast ignited a fire on the nearby highway. Damages were estimated at $1 million (or more than $2,700,000 in 2015 dollars) (Thomas, 1981). Though the Macheteros group's underlying message was Puerto Rican independence, the focusing event that led to the bombings was the eviction of a squatter village to whom the Power Authority refused to provide electricity (James, 1981; Thomas, 1981).

A series of four attacks along the Oregon and California border in October of 2003 were initially thought to be an act of vandalism, where a man in a pickup truck was spotted several times removing and loosening bolts from high power transmission lines and pylons. Damages were small, no power was lost to the surrounding area, and none of the structures fell. The assailant, Michael Devlyn Poulin, eventually turned himself in within weeks following the attacks, and he asserted to the Associated Press (AP) (in an interview prior to turning himself in) that he was trying make a point that the electricity infrastructure in the U.S. was vulnerable low-level attacks, capable of being carried out by a single person. The AP states that he considered his actions "necessary to highlight critical vulnerabilities to the power infrastructure -- a system that could be breached easily" (James, 1981). Poulin was a member of the anti-war group, the Peace and Justice Action League of Spokane, and he felt that the U.S. was misguided in their anti-terrorist approach to the Middle East when vulnerabilities were still prevalent domestically (Associated Press, 2003).

2.6.5 Attacks as an Act of Vandalism

Attacks of vandalism are distinguished as events where the attacker doesn't have a clear sense of direction; an unclear motive, little to no understanding of the system they are attacking, and possibly not even intending to cause significant, or any, damage. The 12 incidents of vandalism included in the motivation analysis that do have additional details often include statements from authorities that state the incident is being treated as an act of vandalism, rather than something more sinister.

One of the reported incidents with details includes an attack by an unknown vandal, though police suggested the attacker(s) were affiliated with a student radical

group, attacked transformers with firearms at Stanford University on April 23, 1971. There was little to no damage, the attackers were never identified, and no motive was ever presented for the attack (Us, 1971). A more recent example, and one in which the perpetrator most likely did not intend to cause any damage, is the 1998 incident in San Francisco involving 19-year veteran of PG&E, Paul Madronich. Mr. Madronich was arrested for keeping 250 pounds of fertilizer explosives and other bomb making materials in his locker at PG&E. However, police soon concluded that Mr. Madronich was a bomb making enthusiast (his lawyer describing him as a misguided hobbyist), and in 1999, Mr. Madronich received one year in jail and three years of probation (Holding, 1999).

2.6.6 Incidents as an Act of Theft

There are nine reported thefts within the database, all occurring between 2012 and 2014. Theft at electricity infrastructure sites usually is further specified as copper wire theft. Theft of copper wire especially is relevant when prices for copper are high and supply is low. Copper prices peaked in 2011 at $4.57 per pound, which may explain the burst of thievery from electric infrastructure during the years that followed. The price of copper has since dropped to $2.52 per pound as of May 2017 (Macrotrends, 2017).

2.6.7 Attacks as an Act of Sabotage Not Otherwise Specified

The final motivational factor indicated in the database is ambiguous. We again rely on additional reporting of the incident by media or other official sources, resulting in only five incidents to assess in the motivation aspect of our analysis. Incidents included in this motive category are ones in which physical destruction of the infrastructure was apparent and differentiated than petty vandalism. For example, on October 31, 2014, more than 2,000 homes in city of Ferguson, Missouri lost power for approximately an hour. While

police report that the incident was vandalism, they also note that the attacker cut a lock and used a specialized tool to disrupt equipment at a specific power pole. The authorities note that this was a highly risky move, and the knowledge to target that location and use the proper equipment indicates insider knowledge of the power grid (Hayes, 2014). Thus, this incident demonstrates more of a purpose rather than general vandalism and is considered sabotage within our motivational analysis.

2.7 Results

The database provides information about the evolution of attacker methodology, motives, and consequences between 1970 and 2016. In total, there are 52 attacks reported by the media, allowing for an in-depth analysis. The data provide information not only in regard to attacker motivation, but also on geographical trends, target types, preferred methods of attack, and potential vulnerabilities of electricity infrastructure that might not otherwise be realized (such as repeated attacks against a single entity or a spree of attacks targeting similar infrastructure). Key findings are presented below, with Figures 1-7 illustrating these trends.

Figure 2-1 present the number of incidents that occurred each year from 1970 to 2016. First, it is observed that attacks were most prevalent from 1970-1999, with 36 attacks, but continued from 2000 to 2016 with 16 attacks. Power stations, substations, and transformers are by far the most targeted energy-related infrastructure, with 30 recorded attacks, as shown in Figure 2-2. Attacks against utility poles, transmission lines, and pylons are the next most targeted infrastructure, with 14 recorded attacks.

In terms of attacks method, explosive is the dominant method of attack against electricity infrastructure, with 30 incidents overall. Physical sabotage or destruction

accounts for 14 incidents, followed by suspicious activity and theft tied with eight recorded incidents each, and lately arson and firearms each used twice. The attack method trends depicted in Figure 2-3 show that explosive devices are used continuously over the decades but theft emerges as more popular methods of attacks after the year 2000.

Utilities, along with federal and local governments, should be vigilant against the possibility of an attack method that uses explosive devices. The catalog of events demonstrate the explosive devices are relatively easy to make or be obtained, and can cause fairly substantial damage in terms of monetary value, service interruptions, and potential threat to human life. Measures should be taken to secure perimeters and/or access to electricity infrastructure, such as at power station, substations, and transformers. Though explosive devices are common, only one recorded incident that involved an explosive device resulted in a fatality, the PG&E substation bombing in May of 1971 (Hewitt, 2005, p. 81). To date, electricity infrastructure attackers seem to attack with the goal of disrupting service or causing commotion, not with the specific intent to inflict injuries or casualties in their attacks. However, attacks using explosive devices do have the potential to cause injury or death, demonstrating that the attackers in some of these incidents were not opposed to violence.

The analysis for attacker motivation allows for incidents to be counted once for each category under which they are classified. This means that an incident is double counted if it is categorized primarily as an attack in protest to a single focusing event and secondarily as an attack against U.S. foreign policy, though all incidents are weighted equally. Instances that fit into this categorization are once in which a specific incident

causes the initial attack (a single focusing event) and results in a group or organization forming and continuing to attack in the name of the initial incident (such as attacking with the goal to disrupt a utility or to protest U.S. foreign policy). Attacker motivation between 1970 and 2016 is depicted in Figure 2-4, 1970 and 1999 in Figure 2-5, and 2000 and 2016 Figure 2-6, for clarity.

Attacks are most often motivated by the desire to desire to disrupt federal and local governments, economies, or utility companies, with 27 total attacks. Attacks in protest to a single focusing event are second most common, with 16 total attacks, followed by media-reported acts of vandalism (12 attacks), and attacks where the intent is theft of utility property (nine incidents). Fifth most common are attacks in protest to U.S. foreign policy or military activity (seven attacks), followed by environmental motivated attacks (six attacks) and, lastly, media-reported acts of sabotage (five attacks). Attacks targeting the disruption of governments, economies, or utilities dominated in the 1970s to 1980s with 21 attacks, while reoccurring only twice throughout the following two decades. Similarly, attacks in protest to a single focusing event were most prevalent in the 1970s and 1980s with 15 total, but then only occurred once more in 1999. In their place rose eco-terrorism, vandalism, attacks in protest to U.S. foreign policy and military activities, and sabotage attacks.

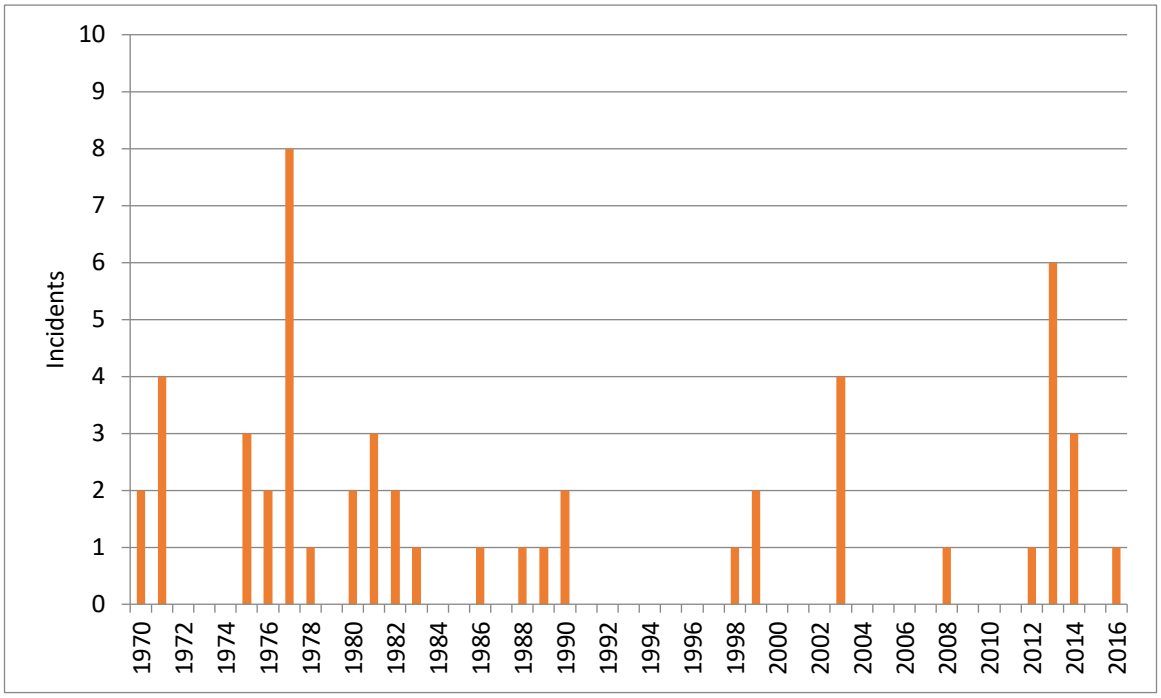

Figure 2-1. Total attacks on the grid, 1970-2016

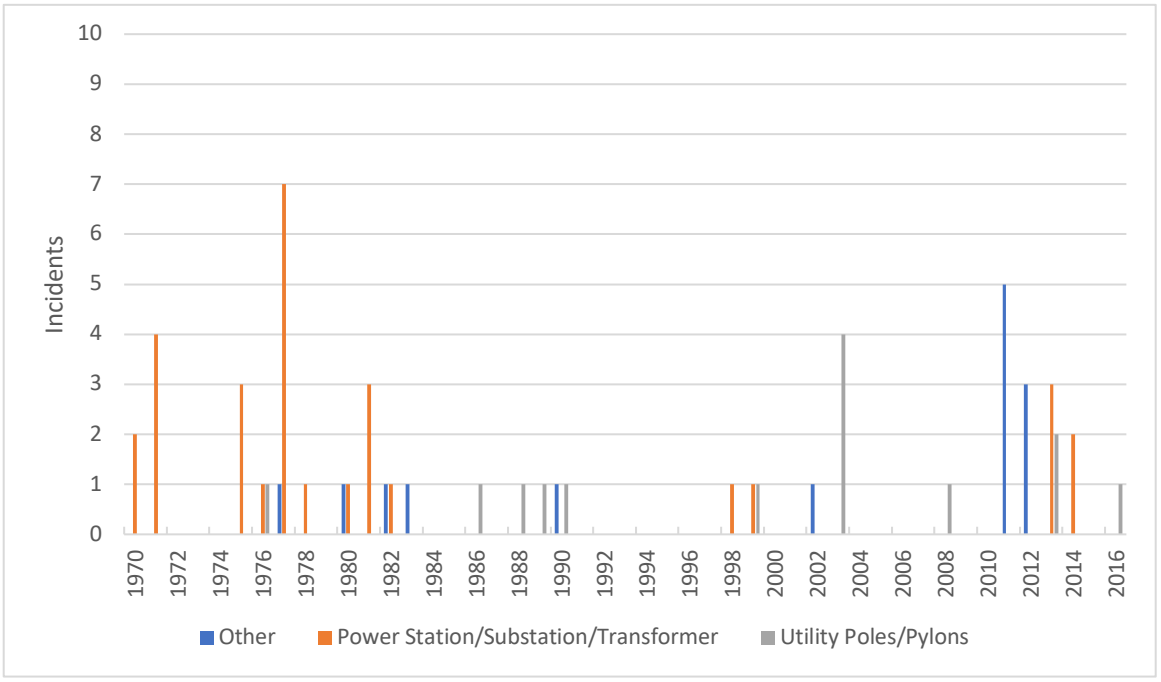

Figure 2-2. Targets of attack on the electric grid, 1970-2016

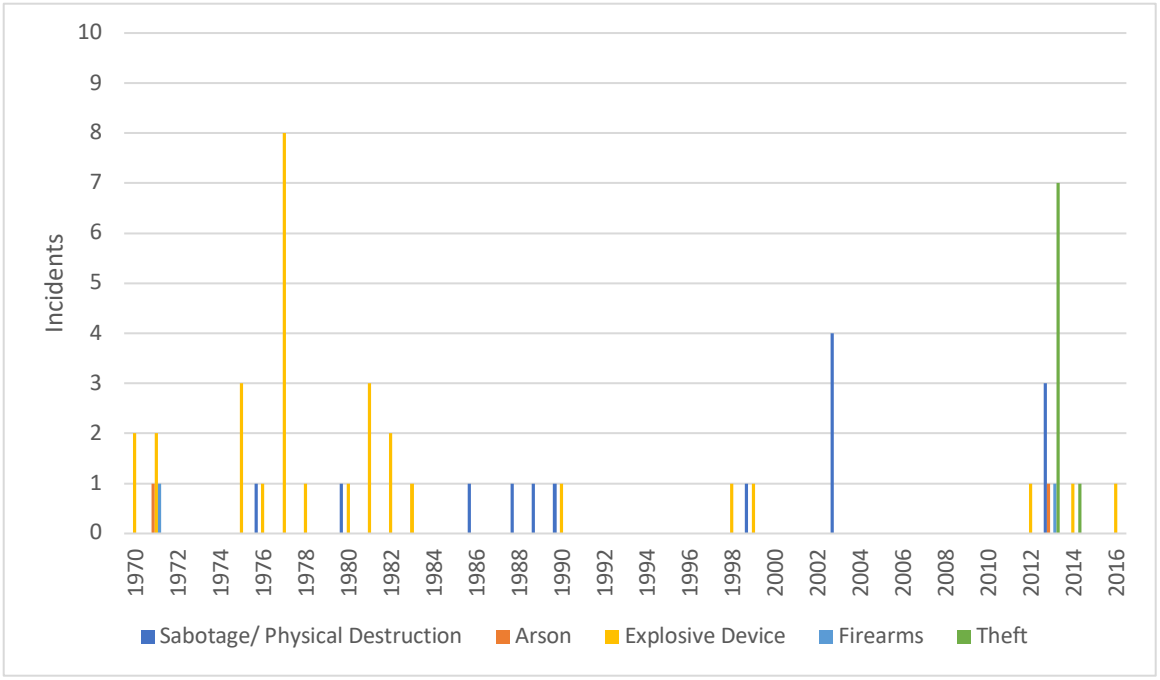

Figure 2-3. Attack methods used to target the electric grid, 1970-2016

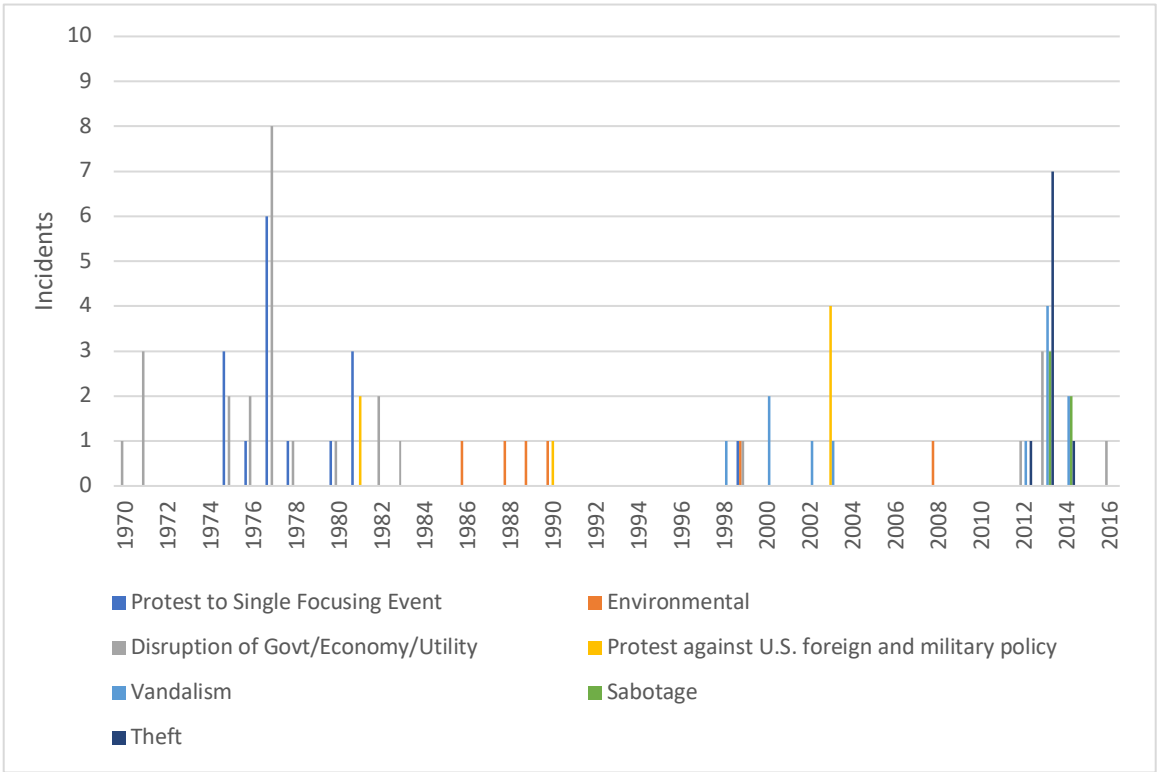

Figure 2-4. Motives for attacking the electric grid, 1970-2016

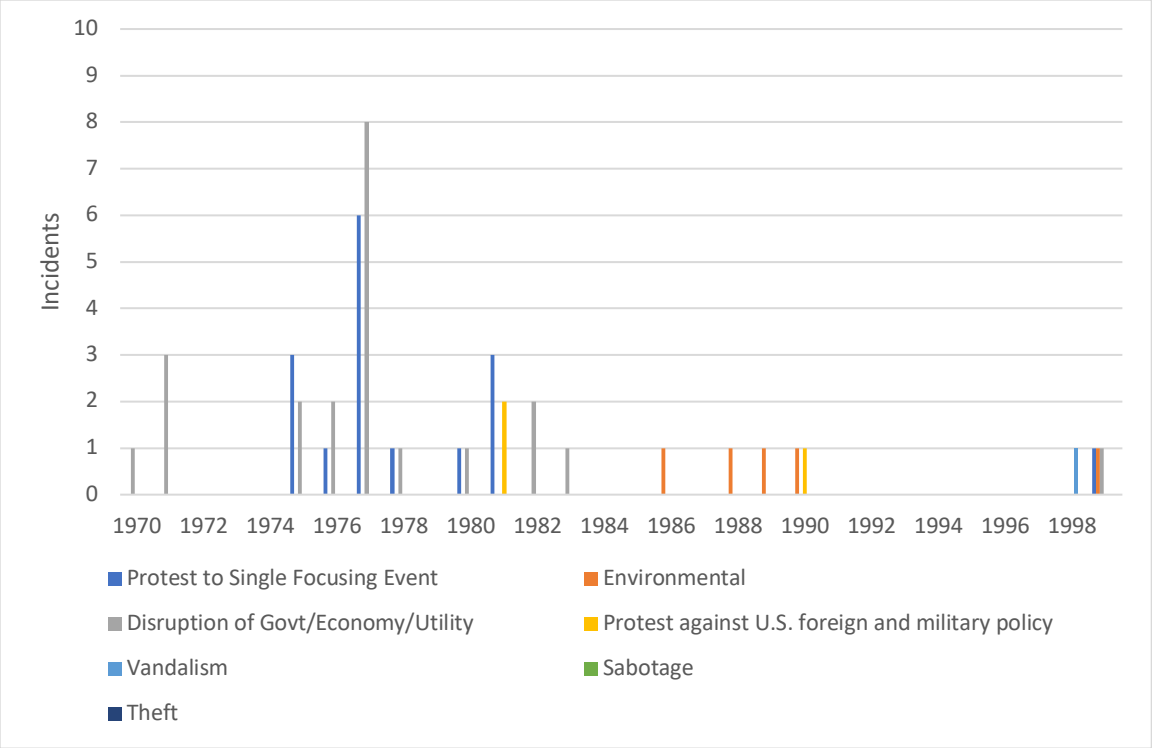

Figure 2-5. Motives for attacking the grid, 1970-1999

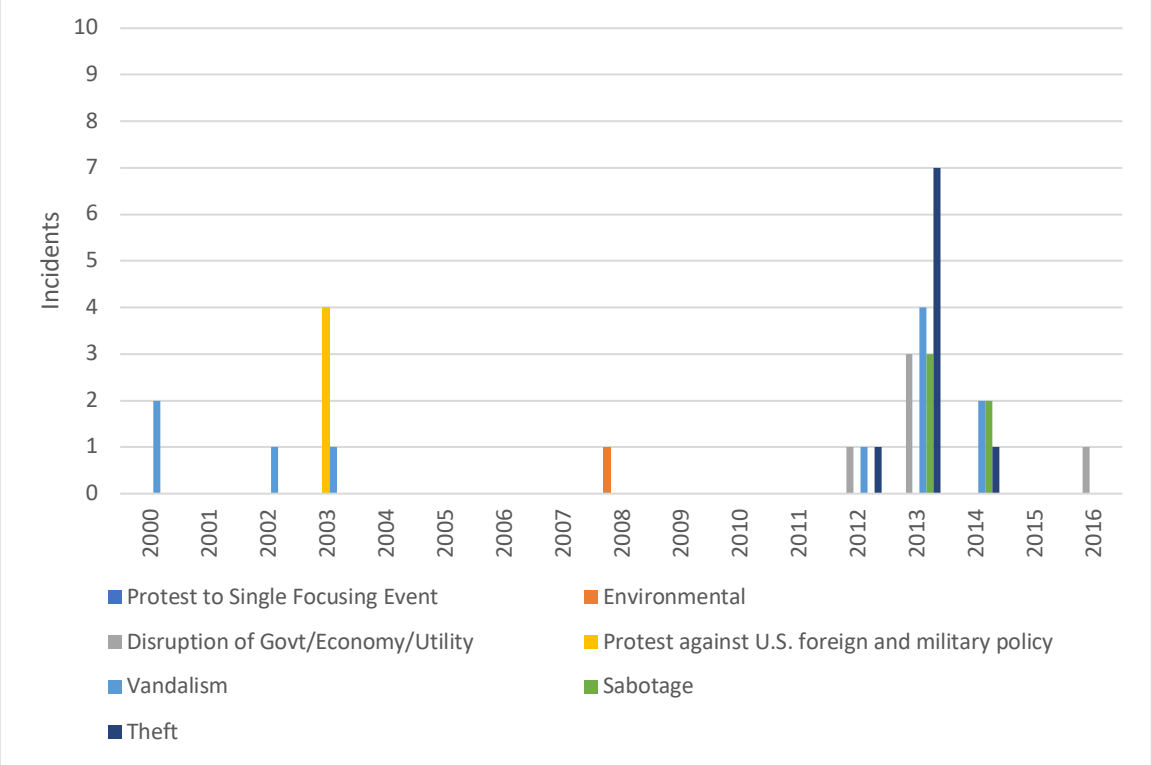

Figure 2-6. Motives for attacking the grid, 2000-2016

2.8 Discussion

Despite action taken by the DOE and DHS to better track unusual disturbances at electricity infrastructure, such as through the OE-417 database, the reporting requirements are too flexible and vague to allow for adequate analysis. Therefore, we must rely on incidents reported in the media. However, the media can also be inconsistent reporting trends though. The media reported on 36 attacks between 1970 and 1999, but only 19 after the year 2000. While there was likely no change in the number of attacks taking place, one notable difference is that attackers began to move away from making the motives for attack known. In the earlier decades included in the database, attackers were motivated to communicate a goal or a message to the society, or coerce the government or private entity to change in some way. Attackers would call or write to local media agencies in order to broadcast the message. In the more recent decades, however, media reported instances drop, and attacker motivation is most often communicated only if the perpetrator is captured. An example of this changing trend can be seen in two different examples of attacks in the California Bay Area against the utility Pacific Gas and Electric. The first example is actually a series of attacks occurring between 1970 and 1980 by an organization called New World Liberation Front (NWLF), and the second example is the Metcalf Sub-Station attack in 2013.

In the early 1970s, the NWLF emerged, with a subset of the organization calling itself Eugene Kuhn, named after a 74-year old resident of Ohio who died of hypothermia following the shutoff of his home's utilities due to an $18 bill that went unpaid ("Page 17 Column 1," 1977). The NWLF rallied around Kuhn's death and specifically targeted

utilities, demanding that electrical power be free for the poor and elderly. The NWLF relayed their message to local newspapers and radio stations ant the focusing event of Kuhn's death eventually turned into the overarching NWLF aim to influence local government and utility's policies towards the disadvantaged. Eleven attacks on electrical infrastructure are attributed to the New World Liberation Front: by 1978, the organization has detonated nearly 60 bombs against a variety of critical infrastructure (Lebdetter, 1978). Attacks overwhelmingly targeted Pacific Gas and Electric, though the NWLF detonated an explosive device outside of Oregon's Trojan Nuclear Power plant in 1977. While only two attacks caused damage greater than $1 million, nearly all attacks caused property damage of some sort. Service interruptions also occurred and ranged from 8,000 to 25,000 homes without power in the aftermath of such attacks.

New World Liberation Front is also responsible for the peak in attacks using explosive devices in the 1975 to 1980 timeframe. Only one of the 11 recorded incidents of a NWLF attack involved physical sabotage, while the rest were attributed to explosive devices. Nine out of 11 attacks targeted power substations, while the one physical sabotage attack was against utility poles and the remaining explosion was the incident outside of Trojan Nuclear Power. The NWLF organization stayed local in their attacks, only targeting the regional electricity provider, Pacific Gas and Electric (PG&E). Though the number of attacks carried out by the NWLF is plentiful and the organization did succeed in causing service interruptions and fairly substantial monetary damages, the NWLF is still not classified as a Sophisticated or Coordinated attack. This classification is due to the attitude of investigators towards the group during that time period. After a 1978 bombing at PG&E substation, the FBI bombing coordinator, Frank Daniel, told the

New York Times that "It's sheer, dumb luck on their part," that the NWLF attacks had any success in causing service interruptions ("Terrorist Unit Resurfaces, Claims Power Plant Blast," 1978). There is no indication that PG&E took steps to improve security at its infrastructure, nor is there any indication that the company ever gave in to the demands of the NWLF. The time period in which these attacks happened, however, is a limiting factor in being able to solidly claim that PG&E did nothing to counter the attacks.

The second example is the Metcalf Substation attack, owned by Pacific Gas and Electric (PG&E) in San Jose, CA. Attackers fired at the substation with automatic weapons for 19 minutes, before retreating just as police arrived. The attack damaged 17 transformers and spilled 52,000 gallons of oil from a storage tank on site. Damages are estimated at $15 million, the most expensive of any event in the dataset, and the substation was out of service for 27 days, requiring electricity to be rerouted to the surrounding Silicon Valley (Smith, 2014b).

While the motives of the attack or whether it was a terrorist incident remains unknown (the Federal Bureau of Investigation (FBI) asserts that it was not a terrorist attack)(Serrano and Halper, 2014), both FERC and PG&E were understandably alarmed by the event. The attack occurred at 1:00am the night after the Boston Marathon bombings, prompting suspicion that the attackers took advantage of a distracted nation and that this attack was a test run for more to come (though there is no evidence to support this claim) (Serrano and Halper, 2014). Despite being described as a relatively low-tech attack, the incident was a well-coordinated event with attackers staying out of view from security cameras and aiming at the substation (though not at the most critical

part of the system) (Serrano and Halper, 2014). Again, as emphasized both in previous research and by the former CIA director, attacks targeting specific critical yet vulnerable infrastructure do not need to be highly technical in order to cause widespread outages (Register, 2015; Sovacool and Brown, 2010).

What is notable about this specific attack though is first, that the attackers knew where to position themselves to avoid the security camera and were able to escape the area before police arrived on the scene. Second, it is notable that this incident still remains unsolved. Unlike the numerous attacks of the 1970s and 1980s, no one called into the local radio stations or newspapers, nor were any notes left onsite communicating why the substation might have been targeted. Instead, investigators are left to infer what the goal might have been. A possible explanation for the attack is that the perpetrators were aware that transformers are some of the most critical infrastructure for power distribution, and also some of those most difficult to replace. There is a shortage of spare transformers and many can only be transported via specific railcars or trucks, leading to a long time lag between a transformer's breakdown and replacement installation (National Research Council of the National Academies, 2012; Salmeron et al., 2004).

This event did, however, directly lead to the mandated North American Electricity Reliability Corporation (NERC) critical infrastructure protection (CIP) standard (CIP-014-1), which was finally approved by FERC in January of 2015, though had been in revision since 2006. The CIP requires utilities and operators to meet new standards for the physical security of electricity infrastructure and, with collaboration from the Department of Homeland Security, offers guidance to for federal and local governments to work directly with the utilities to improve security (NERC, 2014).

Additionally, in December of 2014, Pacific Gas and Electric declared that the company would spend $10 million between 2015 and 2018 on improving the security of the company's infrastructure and technology (Security Sales and Integration, 2014). This pledge to improve security was not a direct result of the 2013 Metcalf substation attack, but rather it was after PG&E was reprimanded for not improving security at that specific substation in the year following the attack. In August of 2014, the Metcalf substation was robbed of $40,000 worth of construction-related equipment. California State regulators have since fined PG&E $50,000 in September 2015, the most the state has ever fined a utility (Associated Press, 2015). Being proactive, Virginia Dominion Resources pledged in 2014 to spend $300 to $500 million over the next 10 years, and other large utilities are said to be following suit (Smith, 2014a).

2.8.1 The Emerging Subset of Sophisticated and/or Coordinated Attacks

The emergence of attacks that move away from clear protest-based motivations and instead appear more sinister in nature, usually indicated by tacit knowledge of the infrastructure subject to attack. We refer to this subset of attack motivation as sophisticated and/or coordinated attacks. Sophisticated and/or coordinated attacks are mostly speculative occurrences, with 11 such instances occurring since the year 2000, as seen in Figure 2-7, including the Metcalf Substation attack.

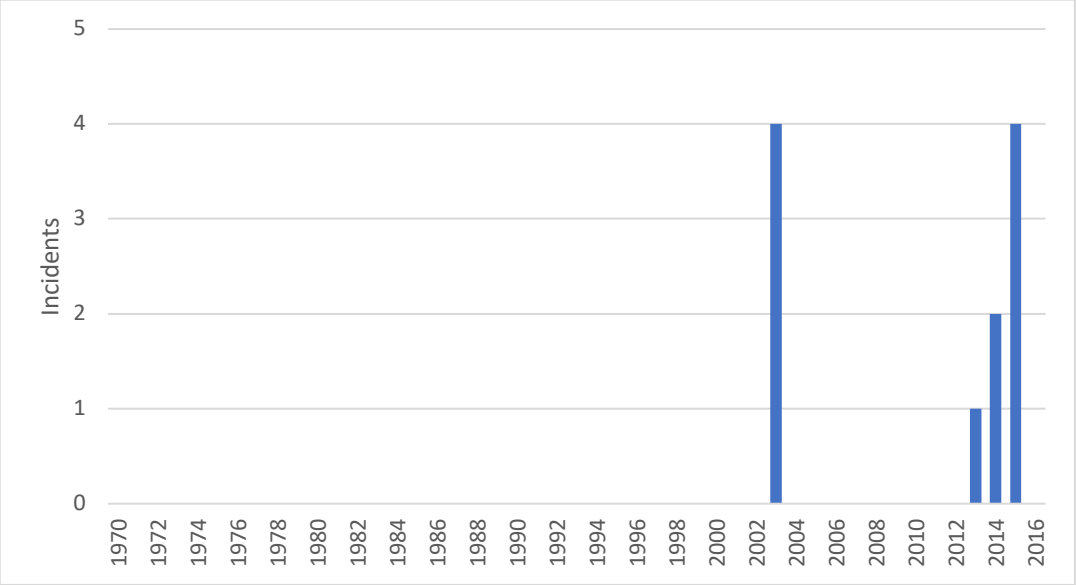

Figure 2-7. Sophisticated and/or coordinated attacks on the grid, 1970-2016

A fear for federal agencies tasked with operating the electric grid, such as FERC and NERC, is an attack that is coordinated across locations or targets and perpetrated by sophisticated individuals with relatively advanced understanding or tacit knowledge of electricity infrastructure. Sophisticated attacks may be similar to attacks of sabotage because the attacking party does not come forward and advertise their motivations. However, the hypothetical intent of the attack is usually seen as more sinister with the goal to cause widespread and prolonged outages or service disruption. Previous research on critical infrastructure vulnerability has noted that attacks often are not considered terrorist attacks unless there are injuries, yet attacker motivations have been evolving to include extensive property damage and disruption (Post et al., 2000). Even now, the FBI does not explicitly include property disruption in their definition of terrorism, despite stating that domestic terrorism can include motivations that "affect the conduct of a government by mass destruction" (FBI, 2018).

While the electricity infrastructure, excluding nuclear, is not considered the most ideal sector to attack to cause widespread destruction or fatalities, an attack of this nature could be coordinated with another, more shocking attack, such as one that causes fatalities or an attack aimed at causing widespread panic amongst the public (National Research Council of the National Academies, 2012, p. 49; Register, 2015). Sophisticated or coordinated attacks of this nature are indeed possible, with the key targets not only being known to potential attackers, but also vulnerable to such attacks. Transformers and high-powered substations that connect the three main interconnections (Texas, Eastern, and Western) may be both the most critical and vulnerable to attack because a failure at these points could result in widespread service outages across the country, plus long repair times due to the lack of readily available spare transformers (Register, 2015; Salmeron et al., 2004; Sovacool and Brown, 2010). As former CIA director James Woolsey stated, if there are multiple interconnection point attacks and outages, "it could be many weeks or months till the system is back to normal. By then, the country could be in chaos" (Register, 2015). The resulting fear of harm, paired with the lack of basic electrical services, could lead to public fear and potentially mistrust of the U.S. government's ability to handle the situation if the power outage is extensive and long lasting (Smith, 2014a).

In terms of attackers actually being able to carry out a successful sophisticated and coordinated attack, researchers note that that a massive outage is not only possible but also not very difficult if a coordinated attack was organized by just a handful of enthusiastic terrorists with access to weather balloons (or drones) and some type of explosive device (Sovacool and Brown, 2010). New attackers could also follow examples

set by their predecessors, such as the Farabundo-Marti National Liberation Front in El Salvador, and publish information manuals explaining how to best to attack power stations and electricity infrastructure (Register, 2015; Sovacool and Brown, 2010).

Sophisticated attacks are a recent occurrence in the database, with eleven incidents since 2003. Of note is Michael Devlyn Poulin's 2003 sabotage attacks of utility poles and pylons (categorized here as sophisticated and coordinated due to the repetition of his actions), specifically intended to demonstrate that the U.S. critical infrastructure was still vulnerable to domestic attacks after September 11. After the Metcalf Substation attack in April, 2013, another example of a sophisticated attack occurred just over a year later, on June 11, 2014 in Nogales, Arizona. An explosive device was placed next to a 50,000-gallon diesel fuel tank, located within the UniSource Energy Services' power station (Holstege, 2014a, 2014b). Although the device detonated, the bomb failed to rupture the tank and damages were less than $1 million. Due to the insider access to the facility, the FBI has been involved with the ongoing investigation of the attack (Homeland Security, 2014). This example again brings up the possibility that knowledge of electricity infrastructure can aid potential attackers, but also a new concern: that terrorists can be well educated, employed, even engineers, as past literature has noted (Clarke, 2004). Though specific details are not known about this 2014 attacker, he or she seems to have been employed by UniSource, given the access to the power station, an a person in this position is likely to have tacit knowledge of the facilities operations. Particularly concerning, and as demonstrated in the September 11 attacks, are engineers that may be recruited or willingly seek out terrorist organizations explicitly because of their education and tacit knowledge (Clarke, 2004). While this might not be the situation

at UniSource, this incident at least serves as a reminder to the possibility of such an attack.

There are fears that attacks will continue to become more sophisticated and coordinated in the future, targeting key infrastructure that will result in widespread and prolonged blackouts. While cyberattacks demonstrate that hacks, viruses, and malware are a present threat to corporations both in and outside of the energy sector, cyberattacks can also potentially reveal critical plant information, including detailed maps and engineering layouts of the plants. This was the case with the 2013 hack against Calpine Corporation, where a cyberattack resulted in the attackers having access to blueprints and detailed information about plant operations (Burke and Fahey, 2014). Attacks of this nature can potentially allow for subsequent targeted cyber-enabled physical attacks, or also provide information for motivated attackers to specifically target certain areas of a power plant or substation.

2.9 Conclusions & Recommendations

It will always be difficult to predict behavior, especially in regard to terrorist and targeted attacks, but a categorical analysis investigating motivations and trends behind past attacks can help. To our knowledge, this is the first database created specifically for the U.S. electricity infrastructure in order to analyze past attack methods, geographical regions, motivations, and other the trends. To cause major damage, the terrorists need to know explicitly where to target, but they will also select targets that are not extraordinarily difficult to access. This is perhaps why so many attacks occur on what eco-terrorists refer to as “soft” targets – ones that are removed from population centers or even alone in rural areas with little to no security (Loadenthal, 2014).

Not until recent years have voluntary security measures evolved into mandatory requirements for utilities and operators, as seen with NERC's newly implemented critical infrastructure protection standards (Shumard, 2015). While collaboration between large agencies, such as the Department of Homeland Security, FERC, and NERC is necessary to communicate security risk, preparedness, and response, private and public utilities and operators must also be included in the discussions since they are most familiar with their system vulnerabilities. Upgrades to security could not only help mitigate the risk of future attacks, but also to also address the aging infrastructure and improve reliability in the event of a weather-related event that threatens the infrastructure. Substations and transformers are infrastructure that deserves particular attention due to the long time lag to repair or replace the system in the event of an emergency or attack. Funding secured for the security improvements should adequately reflect the potential cost of a large scale, coordinated attack on electricity infrastructure if appropriate security improvements are not implemented. Such an attack is estimated to cost the U.S. economy hundreds of billions of dollars (National Research Council of the National Academies, 2012).

What may have the most potential for success in improving electricity infrastructure security is combined effort of top-down and bottom-up security measures. Because of the vast number of electricity-related infrastructure across the U.S., including power stations, transformers, pylons, and utilities poles, it is impossible to quickly implement widespread security measures to all sites at once. Instead, regulatory agencies, such as NERC and FERC, should focus on addressing key security flaws at the most susceptible, critical, or previously targeted structures. By issuing mandatory security improvements at these sites, federal agencies can begin the processes of comprehensive

security upgrades. Furthermore, a top-down approach is needed to purchase, construct, and distribute spare transformers, seeing as these systems are perhaps the most critical in keeping electricity flowing throughout the country. The inability to quickly identify, transport, and install a spare transformer in the event of a disruption (be it a natural disaster or targeted attack) could lead to widespread outages across a region and inflict damages to society and the economy.

State and local governments and individual utilities should focus on bottom-up security policies. Rather than waiting for mandates or specific guides from federal agencies, these groups should begin to implement their own security improvements and measures. Starting from the bottom-up allows for local and state governments or utilities to assess their key vulnerabilities and risk of certain attacks, as demonstrated through information on past incidents (both targeted attacks and nature-related). While some utilities are already taking steps to customize their security response and upgrades, such as Pacific Gas and Electric and Virginia Dominion, more independent operators and utilities should follow. States with the highest number of historical attacks on infrastructure or damages due to weather and other incidents should also act to improve infrastructure based on their specific needs. California, home to the most targeted electricity infrastructure attacks, should assess counterterrorism policies and standards that can specifically improve California-based infrastructure reliability and security. The Pacific Northwest in general should pay attention to security improvements aimed at addressing the threat of attacks using explosive devices and physical sabotage.

It is in the best interest of states, utilities, and the federal government to either voluntarily or through mandatory measures improve electricity infrastructure security.

Aging infrastructure is one of the most vulnerable aspects of these targets, and addressing age with improvements and technological updates can also help secure electricity infrastructure against targeted attacks, including physical attacks and cyberattacks. The updates will also protect the infrastructure against non-malicious, but inevitable incidents of weather or accidental damage to infrastructure. With the appropriate attention, resources, and funding, the electricity infrastructure across the United States can benefit from modernized security and technology and thus be better equipped to recover from a coordinated and sophisticated attack.

CHAPTER 3. FEDERAL R&D FUNDING RESPONSE TO INCIDENTS ON THE ELECTRIC GRID

3.1 Introduction

Security and reliability of the United States' electric grid is the backbone to well-functioning critical infrastructure across the country. However, the nation's electric infrastructure is neither completely secure nor reliable, and is routinely subjected to failures, outages, and other disturbances. These disturbances may be caused by technical or human errors, by severe weather events, or even by intentional physical and cyberattacks. While not all disturbances cause service disruption or power outages, the vulnerabilities for disruption remain. Between 2000 and 2017, there have been 521 suspected and confirmed incidents of physical sabotage on the grid and 20 suspected or confirmed cyberattacks.

Whether the context is grid resiliency and reliability or national security relating to critical electricity infrastructure, unusual disturbances on the grid may result in policy interventions, in terms of funding and implemented grid-related policies or programs. The goal of this chapter is to explore through statistical analysis how significant or unusual events impacting U.S. electricity infrastructure may influence federal research and development (R&D) funding relating to the electrical grid. This chapter focuses on whether intentional attacks on the grid result in an increase in funding allocations within the Office of Electricity Delivery and Energy Reliability compared to a disturbance caused by weather or technical failures. In other words, does a targeted attack imply a risk to national security, which in turn influences federal funding requests and allocations? Or is funding impacted more by other factors, such as the amount of time the

disturbance lasted, or the number of customers without power? These questions center on risk perception theory, specifically how policymakers consider the characteristics and the causal nature of the incident when proposing and implementing R&D allocations at the federal level. Here, the indicator for risk perception within the policy process is measured from key words from Congressional budgetary allocation Committee Reports that refer to the different types of disturbances on the grid.

This chapter first outlines the general background for electrical grid management in the United States, and past trends in research and development funding relating to energy. Next, literature discussing risk perception theory is used as a theoretical founding for how policymakers may perceive threats to grid resiliency, reliability, and security, leading to the basis of the hypotheses to be tested in this analysis. The data sources and methodology used in the analysis come next, followed by the results of the analysis. The chapter concludes with a discussion of the results and outlook for future related research.

3.2 Background

The United States electric grid is expansive, and as a result is managed and operated by a variety of parties in the federal, state, and private sectors. The private sector consists of over 3,200 investor-owned utilities, public power utilities, and cooperative entities (EIA, 2014). These utilities and entities are responsible for generation, transmission, and distribution of electricity. For investor-owned utilities, the Federal Energy Regulatory Commission (FERC) regulates the generation and transmission, while the states regulate the distribution system. Conversely, the generation, transmission, and distribution systems of public power utilities are regulated by the local governments in which the utilities reside (Hoffman and Streit, 2015). At the federal level, the Department

of Energy (DOE) oversees various programs, research, development, and technology deployment relating to the grid. Within the DOE is the Office of Electricity Delivery and Energy Reliability (OE). The OE's mission is specifically focused on ensuring that "the Nation's energy delivery system is secure, resilient and reliable" and as a result, much of the federal government's grid-related research, development, and deployment funding and initiatives are through this office (Energy.gov, 2017).

Though there are many different sectors involved in ensuring that the nation's electricity generation and transmission is operated efficiently and reliably, the research presented here is focused on exploring only the federal role in grid-related research and development funding. Energy and electricity reliability, resiliency, and security is the cornerstone to the functioning of critical infrastructure across the country, including emergency services, health services, communication infrastructure, and the transportation sector. As will be discussed in the Data and Methodologies section, the fiscal year budget and allocations for the Office of Electricity Delivery and Energy Reliability will ultimately be the focus of the statistical analysis. This focus is motivated by an attempt to capture federal-level R&D programs and funding allocations that are influenced by a perceived threat to national security.

As it is difficult to obtain consistent local and state-level policy or funding initiatives relating to electricity infrastructure improvements, annual funding allocations to the OE serves as a way to understand federal policy priorities concerning the grid. This approach comes both from the accuracy and reliability in fiscal year federal budget and allocations reports, as well as from existing literature on the importance of federal funding for energy-related research and development. Studies have directly linked the

amount of federal R&D funding to resulting innovations (Kittner et al., 2017; Margolis and Kammen, 1999; Nemet and Kammen, 2007; Sterlacchini, 2012). Government funding in R&D is a crucial component to bring new innovations and technologies out of the laboratory and into the private sector to be commercialized (Nemet and Kammen, 2007) because often the private sector does not invest in the necessary basic and initial research (Anadon et al., 2017).

However, federal energy research and development spending has been decreasing for decades, despite an increase in the total federal R&D budget (Kittner et al., 2017). Researchers have long viewed this underinvestment as an alarming problem that could impact the nation's ability to adapt to a changing energy landscape, including addressing emerging problems (such as cyberattacks) (Margolis and Kammen, 1999). A recent study focusing on the DOE's Advanced Research Projects Agency – Energy (ARPA-E) program analyzes the issues of appropriations underinvestment from a program evaluation perspective, and concludes that federal R&D funding for the DOE APRA-E program is successful at creating new technology as well as contributing to basic scientific knowledge (Goldstein and Narayanamurti, 2018). While many aspects of electricity infrastructure are operated and regulated by private entities and local or regional agencies, this analysis utilizes federal R&D funding as a measure of policy priorities for the grid. This is with the understanding that federal R&D funding is an important attribute for research innovation on emerging issues, such as those facing the grid.

3.3 Risk Perception Theory and Hypotheses

Does a perceived risk, to personal safety, health, or national security, influence the amount of attention on a specific subject, and subsequently funding allocations towards that area? Studies focusing on risk perception have been used to assess the public's understanding and perception of risks (Akerlof et al., 2013; Bostrom et al., 1994; Leiserowitz, 2006; Leiserowitz and Smith, 2017), reaction to "unnatural risks" (Sjoberg, 2000), and how cultural theory in general relates to risk perception and management (Atman et al., 1994; Rippl, 2011; Wildavsky and Dake, 1990). Research has found that stakeholders must properly understand the problem at hand before they can comprehend whether or not the risk is relevant (Bostrom et al., 1994), with communicating the risk to the stakeholders being a key component of risk perception (Atman et al., 1994). If a given risk is not properly explained or communicated, the stakeholders will be unable to perceive the risk. Policymakers may not choose to act on an increase in number, type, or severity of disturbances on the electrical grid if they are not aware that the events are taking place. It has been found that misunderstandings about terminology and causes related to the risk can lower one's perception of the risk (Bostrom et al., 1994). Conversely, however, it is possible for stakeholders to consider something a risk because the risk is inherently known to be a threat (such as war or threats to national security), regardless of knowledge about the threat (Wildavsky and Dake, 1990).

Having some sort of experience with a given threat or its impacts strongly influences a stakeholder's perception of risk (Leiserowitz, 2006). The stakeholders who experience a certain threat can subsequently communicate about and advocate for a wider understanding of the perceived risk to their social circles, which can lead to a larger

number stakeholders who consider that factor as a risk (Leiserowitz and Smith, 2017). Therefore, concerns about grid resiliency, reliability, or security should be tied with whether stakeholders (here, Congress members and their constituents) have been impacted by disruptions on the grid caused by extreme weather, human or technical errors, or targeted attacks. An increase in concern over perceived "unnatural risks," meaning risks that are immoral or aimed to disrupt with systems, have been shown to increase the level of concern over a given threat (Sjoberg, 2000). Threats associated with terrorist acts, such a malicious attacks, are also associated with potential overreaction by public officials and private citizens alike (Slovic and Peters, 2006).

Based on the existing risk perception literature, will policymakers be more concerned over malicious attacks to grid infrastructure, indicating a threat to national security, rather than events caused by severe weather or technical failures, and subsequently allocate more R&D funding? Figure 3-1 outlines the basic process to be tested in this analysis. The risks, defined here as disturbance caused by weather events, technical or human failures, and malicious attacks, impact the electric grid. Whether policymakers are aware of the disturbances and perceive these disturbances as risks will be indicated by the language used within the House and Senate Appropriations Committee Reports, specifically the frequency of keywords associated with each risk type. In turn, the level of risk perceived is indicated by the policy response to the risk – as shown by an increase in funding to the Office of Electricity associated with an increase in those risks occurring on the grid.

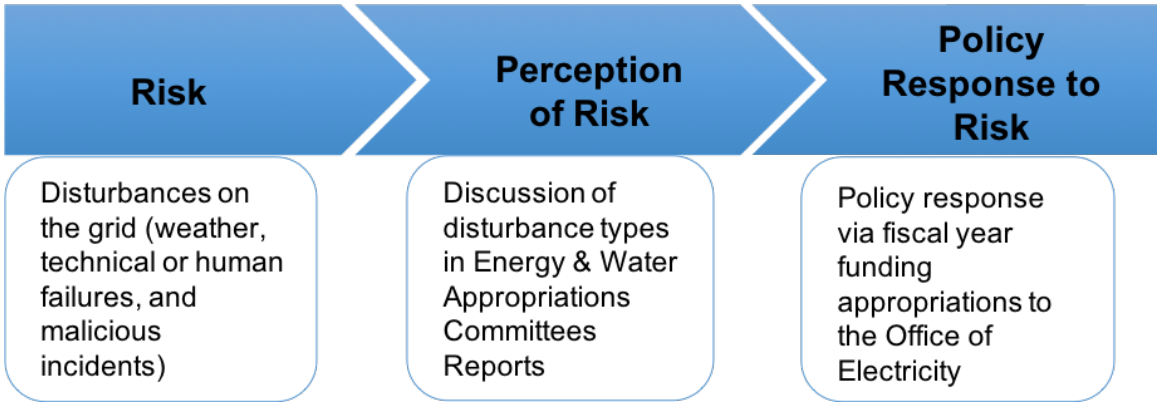

Figure 3-1. Risk Perception Process. Do risks predict Congressional discussion, which in turn predicts funding response?

Following this process outline, the following hypotheses seek to determine whether risks predict Congressional discussion, which in turn predicts funding response. A mediational hypotheses model is utilized here to test the causal relationships between risks that disrupt the electric grid, Congressional discussion of said risks, and the measurable outcome in terms of federal funding for the grid. The first hypotheses tests for an association between the causal variable, risks (disturbances on the grid), and the outcome of subsequent policy response (fiscal year funding levels).

> **Hypothesis 1:** An increase in malicious risks will lead to an increase in appropriations for the Office of Electricity.

The second hypotheses tests for an association between the causal variable, risks, and the mediating variable, discussion about risks to the grid within the Congressional Appropriations Committees Reports. By measuring the frequency of keywords that specifically relate to each risk type, Hypothesis 2 serves as an indicator of risk perception, thus establishing the link between disturbances and policy priorities from the Appropriations Committees. In this analysis, four keywords are assigned to each risk type

in order to count both consistent terminology as well as emerging buzzwords. Additionally, both the House and Senate Appropriations Committee Reports are used so as to capture federal policy priorities that may be influenced from a more local, state- and regional-level perspective.

Hypothesis 2: An increase in risks that are (a. malicious risks, b. tech/human failure risks, c. weather risks) will lead to an increase in discussion of that risk type (a, b, or c,) in the Senate and House budget appropriations Committee Reports.

To then measure the final outcome, the level of policymaker's risk perception to intentional attacks (and thereby threats to national security), the third hypothesis focuses on the relationship between the number of malicious disturbances on the grid and the subsequent policy response (fiscal year funding levels), controlling for the mediation of Congressional discussion (Committee reports). If there is an increase in discussion about malicious attacks or threats to the electricity infrastructure, do policymakers then perceive this risk as a high priority, and allocate more funding to the Office of Electricity?

> **Hypothesis 3:** An increase in risks impacting the grid, controlling for Congressional Discussion, leads to an increase in Office of Electricity fiscal year funding.

3.4 Data and Methodology

3.4.1 Disturbance Database Description

The Department of Energy and the Department of Homeland Security (DHS) often have overlapping initiatives and goals, resulting in crossover programs. A DOE-DHS program pertinent to this research are the reporting requirements and subsequent

database of Electric Disturbance Events. The Electric Disturbance Events database, also referred to OE-417 database and to be described in more detail in the Data and Methodology section, requires utility owners and operators to report any instances on the grid that are unusual in nature; whether that be from a major weather event to a technical error to an unexpected voltage surge, regardless of if an outage is reported. Additionally, any suspected or confirmed physical or cyberattack is required to be reported (Office of Electricity Delivery & Energy Reliability, 2018a).

It is useful to consider how widespread disruptive incidents on the grid are. Using the DOE's Electricity Disturbance Database (referred to as the OE-417 report database), the focus of this analysis is narrowed to grid-related disruptions that are deemed uncommon, unusual, or severe, and therefore required to be reported to the DOE (Office of Electricity Delivery & Energy Reliability, 2018a). Disturbances are reported by utilities, reliability coordinators, and balancing authorities if any of the following criteria are met: interruptions due to a physical attack, interruptions due to a cyberattack, operational failure or shut-down of transmission or distribution, islanding during a blackout, an uncontrolled loss of at least 300 megawatts for 15 minutes or more, emergency load shedding of at least 100 megawatts, voltage reduction of at least three percent, or a public request to reduce electricity on the system (Office of Electricity Delivery & Energy Reliability, 2018a). Reports are required within one to six hours of the incident, depending on the cause, plus an update report and a final report within 72 hours of the disruption (Office of Electricity Delivery & Energy Reliability, 2018a). Though the OE-417 reports are not intended to capture every day, low level disruptions on the grid, the database still indicates that disturbances and disruptions are quite

common and are caused by a variety of factors ranging from weather and nature, physical and cyberattacks, or technical and human errors. The DOE states that the unusual disturbance reports are collected to fulfill "…overall national security and Department of Homeland Security's National Response Framework responsibilities" as well as to be taken in consideration for future policy interventions (Office of Electricity Delivery & Energy Reliability, 2018a).

Because in depth records of incidents and disturbances on the U.S. grid are not readily available for the years prior to 2000, this part of the analysis will only include observations from 2000 to 2017. Although reporting of unusual events that meet the criteria described above are mandatory, these requirements were not always strictly enforced, as evident in the early to mid 2000s of the OE-417 database (Fisher et al., 2011). Comparing the mandatory OE-417 database to a non-mandatory NERC reporting database (that has since been retired and is no longer accessible), the OE-417 database is missing approximately 30 unusual disturbances (caused by weather, failures, or malicious incidents) each year between 2003 and 2005, 20 in 2006, fewer than 10 in 2007, until the two databases match beginning in 2008 (Fisher et al., 2011). To supplement potential loss of malicious attack data, the attack database from this dissertation's second chapter is included in this analysis as well. As discussed in Chapter 2, the attack database requires at least two sources of media reports, governmental reports, peer reviewed journals, and books for the incidents to be included.

The incidents included in the OE-417 reports, as well as the supplemental data from this dissertation's second chapter, are all either highly unusual, high impact, or received high attention, either from the media, regulatory agencies, or industry. Between

the years 2000 and 2017 there have been 2,228 reported unusual disturbances on the grid. As shown in Figure 3-2, 1,093 incidents are caused by weather or nature-related disturbances, 551are caused by suspected or confirmed intentional attacks (with 20 being cyber-related), and 582 are caused by human or technical errors, such as distribution interruptions, fuel supply deficiencies, incidents of islanding, system operation errors, and other causes (such as public appeals for demand reduction). Figure 3-3 displays the yearly occurrences of these disruption incidents.

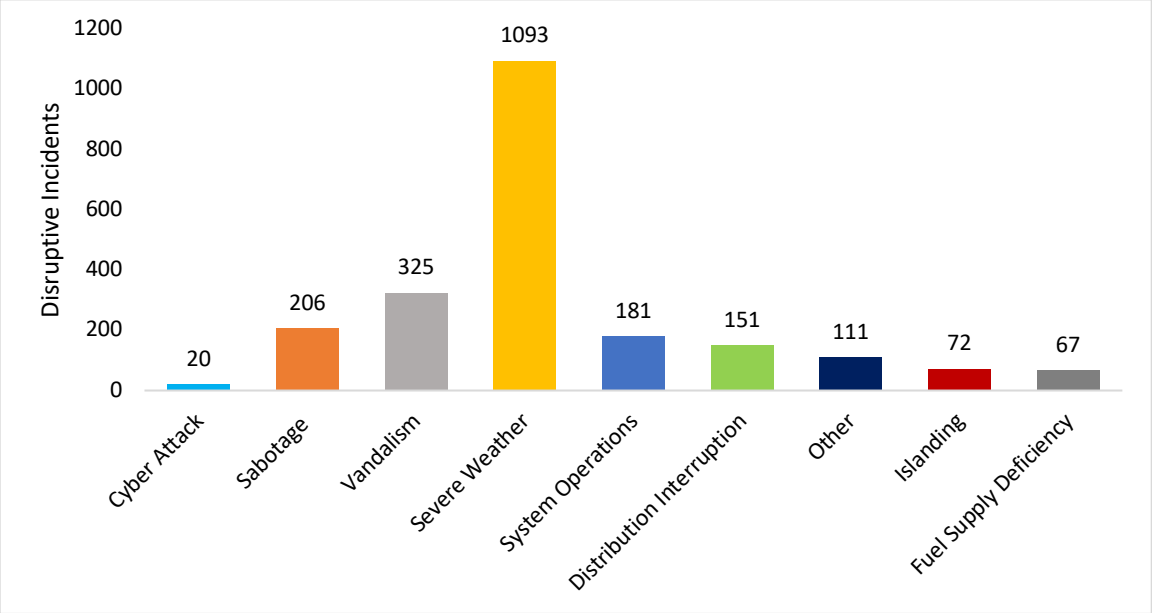

Figure 3-2. Total Number of Disturbances on the U.S. Grid, 2000-2017

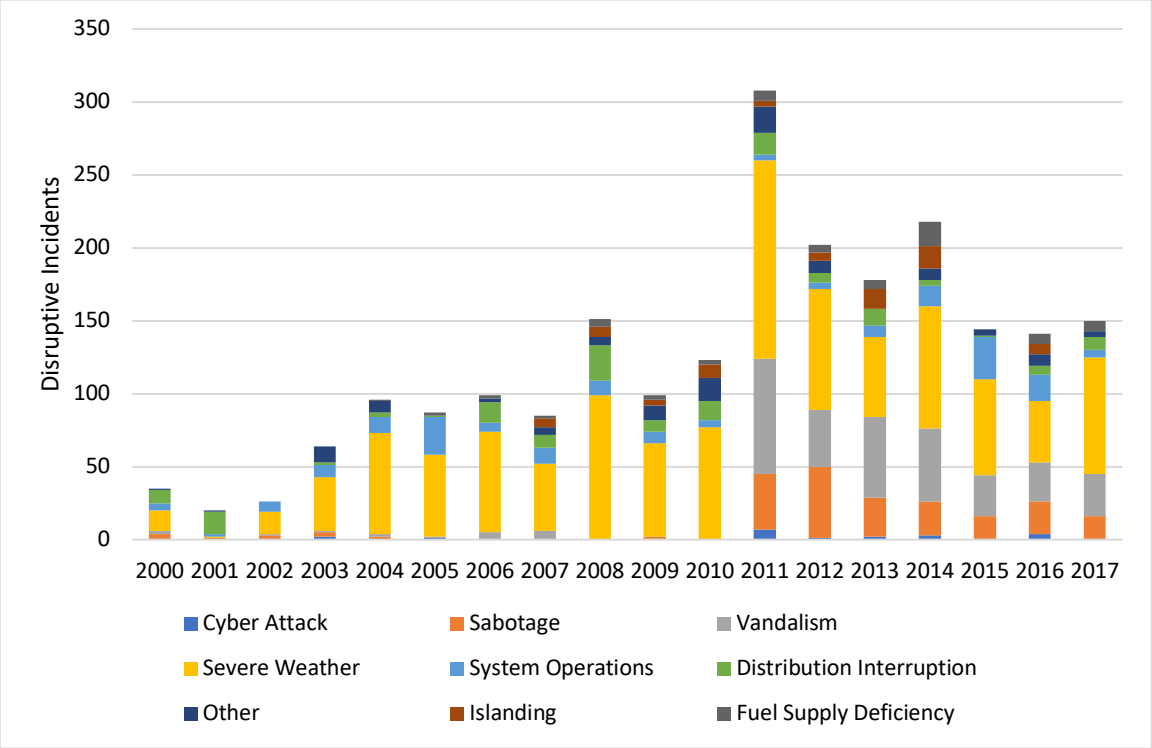

Figure 3-3. Total Number of Disturbances on the U.S. Grid per year, 2000-2017

While it is mandatory for utility owners and operators to report unusual disturbances to the OE-417 database (Fisher et al., 2011), it is unclear as to why there is an increase in reported incidents over the years, seemingly to begin with the spike in reported incidents in 2011. It is possible that, due to the age of the electric grid, the infrastructure is deteriorating and is less resilient to unusual disturbances, especially as more severe weather events are observed (Campbell, 2012). This does not explain the increase in malicious incidents being reported during this timeframe and therefore additional investigation into the OE-417 data reporting requirements is underway.

Acts of sabotage remain a consistent threat to the grid in recent years, as is the possible threat of a cyberattack. There is a prevalence of copper theft being from electricity infrastructure being reported mainly between 2009 to 2013, which correlates to high copper prices around that time (Macrotrends, 2017). Theft is categorized in the OE-

417 reports by utility operators and owners as "vandalism." For ease of analysis, "vandalism," "sabotage," and "cyberattacks" are summed together from this point forward into an overarching "malicious" categorization, with Figure 3-4 providing a closer view of malicious incidents reported since the year 2000. There is a period of time in the mid 2000s where there are few malicious incidents being reported. The attack database from Chapter 2 is merged with the OE-417 database for this analysis for robustness, but also as a mean of supplementing the potential missing data in the mid 2000s. The supplementary attack data merged with the OE-417 database fills in some missing malicious attack data, but attacks being reported remains low during this period.

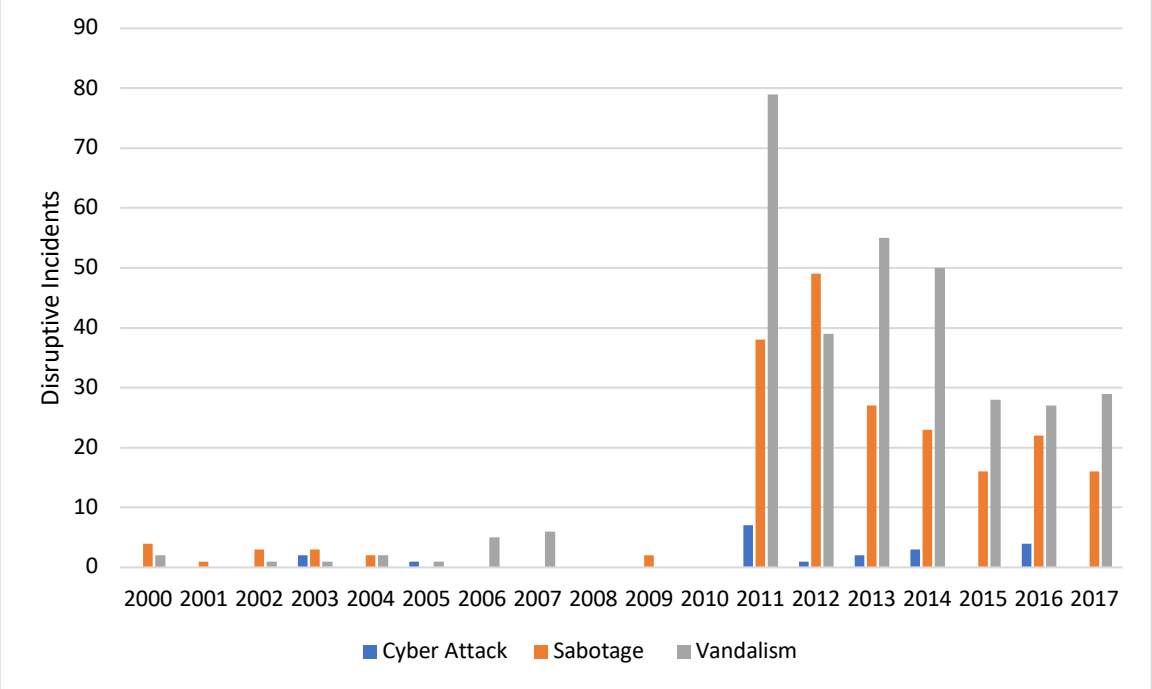

Figure 3-4. Total Number of Disturbances Caused by Malicious Events on the U.S. Grid per year, 2000-2017

3.4.2 Office of Electricity Funding Allocations Description

The private sector, states, the federal government, and NERC all oversee grid resiliency, reliability, and security in various manners and therefore all have inputs and programs aiming to address disturbances such as these. But given that federally funded

R&D programs are vital to addressing emerging trends (Margolis and Kammen, 1999), the focus here is how the federal R&D budget for the DOE's Office of Electricity Delivery and Energy Reliability responds to these types of disturbances over the years. Historical data for the DOE and OE's budget allocations comes from the American Association for the Advancement of Science (AAAS) Historical Trends in Federal R&D database (AAAS, 2018). The OE's allocations within DOE's annual budget includes projects and programs focused on improving grid reliability, resiliency, and security. Initiatives include Smart Grid investment programs, work force training programs, state assistance on electricity policy funding, and programs aimed at enhancing state and local government energy programs (Office of Electricity Delivery & Energy Reliability, 2018b). Manually excluded from the OE funding is the High Temperature Superconductivity program, from 2004-2009, as its research initiatives were out of character for the Office of Electricity.[1]

The organizations that receive funding for both applied and basic R&D projects and programs through the OE include national laboratories, universities, as well as private companies (Goldstein and Narayanamurti, 2018). The federal R&D funding used in this analysis spans from 2003 to 2018, as fiscal year funding for the OE was not allocated until the year 2003. While the database does provide the NERC region of the outage, reporting requirements changed multiple times over the 17-year time period, meaning that names of the NERC regions are inconsistent and unreliable, therefore were not used in the analysis.

[1] Per guidance by Dr. Marilyn Brown, School of Public Policy, Georgia Institute of Technology (September, 2018).

Figure 3-5 displays the fiscal year allocation for the entire DOE R&D compared to the R&D in the Office of Electricity within the Department, with markers indicating major incidents. All monetary data is displayed in millions of current 2018 dollars. Major incidents, such as the Northeast Blackout, Hurricanes Katrina and Sandy, and the 2013 Metcalf Substation Attack, are the kinds of events this analysis is focused on investigating to see if they lead to an increase in R&D funding.

The funding for OE R&D shows peaks in 2006 and 2010 and increases in years 2015 through 2018. The peak in 2006 is attributed to an increase in electricity infrastructure funding included in the 2005 Energy Policy Act, which addressed many issues associated with the 2003 Northeast Blackout, such as cascading failures (109th Congress, 2005). Following the 2008 financial crisis, the additional funding spike in 2010 is from the American Recovery and Reinvestment Act (ARRA) of 2009, which also included policy priorities to address electricity delivery and reliability (111th Congress, 2009; Sissine, 2015). Increases in 2016 included a new transformer resilience program and increases in the smart grid and cybersecurity programs. While DOE R&D funding decreased annually between 2010 and 2014, including within the OE, there was a substantial increase in funding for DOE R&D in 2015, and substantial increases in OE R&D allocations in 2014, 2015, and 2016. Some of the increase in funding in 2015 is reported to have come as a response to the Metcalf attack of 2013, which caused a major stir within the electricity industry as well as NERC (prompting new security mitigation and risk reporting requirements) (North American Electricity Reliability Corporation, 2015a; Shumard, 2015; Smith, 2014a).

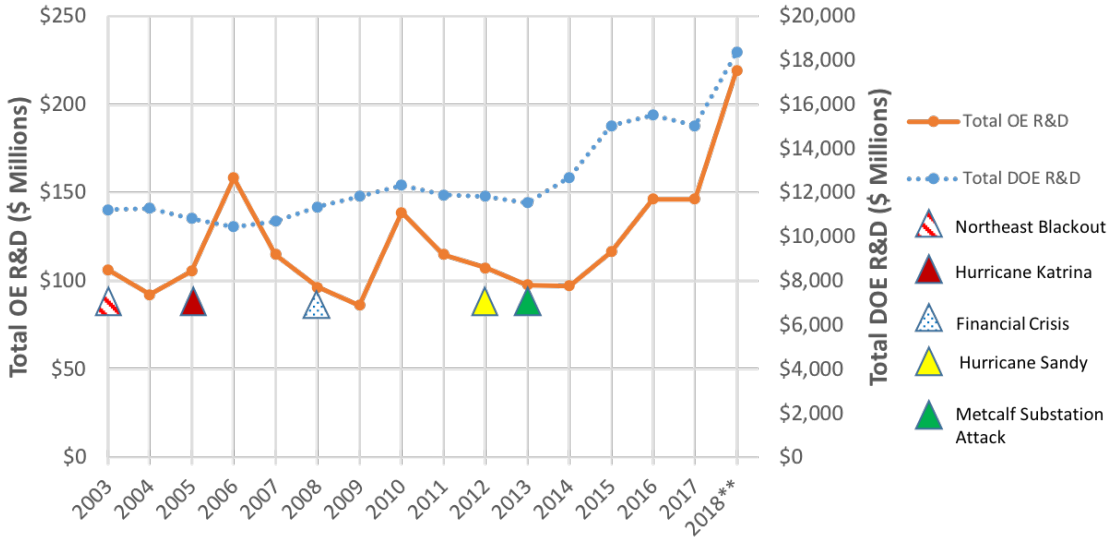

*Figure 3-5. DOE & DOE Office of Electricity and Energy Reliability R&D Fiscal Year Budgets, in Millions $2018 **Discretionary budgets, include non-R&D components **Latest estimates, FY 2017 is the President's request* (AAAS, 2018).

3.4.3 Committee Report Description

The Committee Report data comes from the House and Senate Committees on Appropriations for Energy and Water Development Appropriations (Congress.gov, 2018). Appropriation Committee Reports are released in the early summer months, after the President's budget request in early February. The Committee Reports come after multiple hearings and subcommittee meetings, in both the House and Senate, on issues related to the subcommittee's agenda. While the final Appropriations bill, finalized in identical text by both the House and Senate and then signed by the President, is legally binding, the Appropriations Committee Reports indicate congressional direction through both legally and non-legally binding language. Here, Congress indicates the policy priorities the agencies are to follow with the funding allocations. In an interview, a Senior Advisor in a related agency stated that the message conveyed to the agencies from the

Committee Reports is where policymakers believe the budget will be best spent to focus on risks as well as R&D.

This analysis focuses on the House and Senate Energy and Water Development Appropriations Committees. These Committees cover budget allocations for the DOE as well as the Department of Defense, the Department of Interior, and other Independent Agencies. In this analysis, only the introductory, DOE Appropriations, and concluding sections of the reports are used in the keyword search. Within the DOE Appropriations section, subsections concerning programs other than the Office of Electricity (such as Energy Efficiency and Renewable Energy, Nuclear Energy, Weapons Activities, etc.) are not included. While these sections often include the keywords of interest, the context is often not relevant to improving the resiliency, reliability, and security of the grid. When the overlap between programs within the DOE is relevant, the keywords accounted for in the Committee Report's introductory and concluding sections, as well as sections dedicated to cross-cutting initiatives. Strictly text mining through sections of the reports concerning Office of Electricity funding allows for a more clear cut focus on congressional electricity infrastructure policy priorities. The Committee Reports used in this analysis begin in the year 2003, with the creation of the Office of Electricity within the DOE, and end in 2018 with the current enacted budget. In addition to the annual Energy and Water Development Appropriations Reports, Committee Reports for two other high-profile funding allocations are also included. These are the 2005 Energy Policy Act and the 2009 American Recovery and Reinvestment Act.

3.5 Methodology

Following risk perception literature, this analysis first seeks to determine whether risks such as weather events, technical or human caused failures, and malicious attacks are a perceived risk for Congressional policymakers, as indicated by the language used in the House and Senate Energy and Water Development Appropriation Committee Reports. Next, the analysis investigates whether the cause of an unusual disruption on the U.S. electric grid has an impact on federal funding allocations, as directed through the DOE's Office of Electricity Delivery and Energy Reliability, aimed at strengthening electricity infrastructure.

The three hypotheses being tested in this analysis follow the mediation hypotheses model (Baron and Kenny, 1986; Judd and Kenny, 1981). Using this model, the first hypothesis serves to indicate an association between the causal variable, risk, and the outcome, funding. The second hypothesis severs to demonstrate that the causal variable, risk, is also associated with the mediator variable, Congressional discussion. In the final hypothesis, if the outcome of federal funding is completely controlled by the Congressional discussion, then there should be no statistical significance between risks impacting and funding in this third and final step of the mediation hypothesis model. If there is an effect, indicated by statistical significance, Congressional discussion is only partially influencing funding.

Using a time series regression analysis, the analysis focuses on unusual disturbances on the electric grid between 2000 and 2017, Committee Reports from 2003-2018, and fiscal year funding for the DOE and the Office of Electricity between 2003 and 2018, in millions of 2018 dollars. Though there is a risk of autocorrelation between

previous year's funding allocations and the subsequent year's allocations, a quick check of the trend line for the DOE Office of Electricity funding (Figure 3-5) shows that the risk is low, with an R^2 of 0.2. However, the dependent variable used in Hypothesis 1 and 3 will be the percent of OE funding out of total DOE funding each year in order to further address autocorrelation and keep in mind the relationship between the OE's funding levels within the overarching Department.

An additional factor to consider is that federal funding reaction to disruptions on the grid will not occur in the fiscal year during which the disruptions take place. Instead, any OE fiscal year funding allocations will lag behind the disruptions, as is seen in the federal military fiscal year funding process (Kocherlakota and Yi, 1996). For example, the disruption caused by the 2003 Northeast Blackout might not have an effect on DOE OE funding until the year 2005 (a time lag of two years). While Figure 3-5 shows that major events such as Hurricane Katrina and the Northeast Blackout may have had a funding response of one to two years, funding reported to be responding to the Metcalf Substation Attack did not follow until three years later, in 2015 (Parfomak, 2018; Sissine, 2015). Due to uncertainty about when disruptions may lead to policy change (in this case, federal R&D funding allocations), the regression models below test for a time lag of one to three years.

For the second hypothesis, the frequency of four keywords for each risk type are collected from the Committee Reports and used as the dependent variables *keyword malicious*, *keyword tech-human*, and *keyword weather*. For the risk associated with weather events, the keywords counted are "hurricane," "weather," "climate," and "storm." The word "severe" was also searched in each report, but yielded too few results

to be included. For the risk associated with human or technical failures, the keywords are "reliab" (to capture "reliability," "reliable," etc.), "voltage," "disturbance," and "fail." The word "harden," as in "grid hardening," was also searched but again yielded too few results over the years. Lastly, the keywords counted for malicious risks are "attack," "terror," "cyber" (to capture variations and spellings of "cybersecurity"), and "physical."

*Table 3-1. Total Keyword Count from Energy and Water Development Appropriations Committee Reports, 2003-2018 *Includes Committee Reports for Energy Policy Act **Includes Committee Reports for American Recovery and Reinvestment Act*

	Total Keyword Count, House and Senate						
Year	**Malicious**	**Tech or Human Failure**	**Weather**	**Total Keywords Counted**	**House Majority Party**	**Senate Majority Party**	**Presidential Party**
2003	15	3	1	19	R	D	R
2004	14	10	12	36	R	R	R
2005*	14	272	28	304	R	R	R
2006	8	14	9	31	R	R	R
2007	8	20	14	44	R	R	R
2008	9	21	14	43	D	D	R
2009**	12	22	74	108	D	D	D
2010	10	20	17	47	D	D	D
2011	5	3	1	9	D	D	D
2012	10	19	19	48	R	D	D
2013	7	12	12	31	R	D	D
2014	9	22	17	48	R	D	D
2015	7	12	23	42	R	R	D
2016	17	31	18	66	R	R	D
2017	20	19	13	52	R	R	R
2018	47	27	16	90	R	R	R
Total	**212**	**527**	**288**	**1018**	**-**	**-**	**-**

The keywords were chosen to differentiate between the risk types as well as capture changing language and priorities over the years. The keywords are only counted in the introductory, DOE Appropriations, and concluding sections of the Committee

Reports, and exclude subsections of the DOE Appropriations that relate to nuclear initiatives or activities. Also included as independent variables are *House Majority*, *Senate Majority*, as well as *Presidential Party*, to indicate which political party was in charge of the House, Senate, or Presidential Office each year. These variables are included as binary Republican/Democrat (with Republican being the reference group) to add political polarity to the analysis. Each keyword variable is used in the second hypothesis set, and then included as binary Y/N variables in the third hypothesis. The total keyword count and yearly political majority party for both the House and Senate Appropriations Committee Reports are shown in Table 3-1.

Summary statistics for the disturbance database and DOE funding data are shown in Table 3-2, cumulated in annual totals. The dependent variable of interest, *funding*, indicates the percent of Office of Electricity fiscal year R&D funding out of total DOE funding, lagged *t* years (one to three years) for each model. Disruptions on the grid are coded into the categorical variable *risk*, with the types of risks being malicious incidents, weather-related incidents, and failure-related incidents (as the reference group), in order to test for the impact of malicious events on policymaker's perception of risk. As mentioned, incidents of vandalism, sabotage, and cyberattacks are summed together within the malicious incidents categorization. Similarly, incidents caused by human or technical failures (such as islanding, distribution interruptions, system operation failures, fuel supply deficiencies, or failures otherwise not stated) are summed together as part of the failure incidents. All remaining weather-related incidents are those reported as severe weather incidents.

The independent variable *demand lost* is in gigawatts, and *customer-hours* is the total number of customers (in millions) impacted by the event multiplied by the duration of the disturbance (in hours). The total number of *disturbances per year* is also included as an independent variable and represents the total number of disruptions on the grid per year, as reported by the DOE OE-417 database, regardless of cause. *Media* is included as a binary variable to indicate which disruptions were reported upon by the media and therefore received more attention locally or nationally.

Table 3-2. Summary Statistics of U.S. Electricity Disturbance Database (2000 to 2017) and Department of Energy Fiscal Year Funding (2003-2017)

	Mean	Median	Std. Dev.	Min	Max	No. Observations
Total Incidents, per year	117	99	76	0	308	2228
Malicious Incidents, per year	29	6	39	0	124	551
Weather Incidents, per year	58	64	35	0	136	1093
Failure Incidents, per year	31	30	15	0	58	582
Total Outage Duration (hrs), per year	4606	5289	2895	0	9439	2076
Total Demand Loss (GW), per year	42	40	35	0	119	1240
Total Customers Impacted (millions), per year	13	9	9	0	33	1662
Media-Reported Incidents, per year	11	8	9	0	31	202
Dept. of Energy Fiscal Year R&D Funding ($2018 Millions)	12619	11831	2203	10451	18359	15
Dept. of Energy, Office of Electricity Fiscal Year R&D Funding ($2018 Millions)	103	102	46	35	219	15

As this is a time series analysis, the first important step is creating the Finite Distributed Lag (FDL) models (Wooldridge, 2004, chap. 10), where the data is fitted so each time lag model lines up with the year of interest in which the disturbances take place. Once properly coded and fit, the I use ordinary least squares (OLS) regression models to test each hypothesis across the three different time lag models. Because multicollinearity is a potential issue with time lag models, the number of variables included in the regressions are kept to a minimum (Wooldridge, 2004, chap. 10).

However, collinearity is to be expected between the first and second hypothesis, as the potential relationship between discussion of the risk types in the Committee Reports and subsequent funding is key to this analysis. After incrementally adding in each variable to the regression models and observing that variables with significance remained roughly the same with each addition, the final preferred equations for each hypothesis are listed below.

Hypothesis 1: Risks that are malicious are associated with an increase in appropriations for the Office of Electricity, as a percent of total DOE fiscal year funding.

$$Funding_t = B_0 + B_1\, risk + B_2\, demand\ lost + B_3\, customers\text{-}hours + B_4\, media + B_5\, House\ Majority + B_6\, Senate\ Majority + B_7\, Presidential\ Party$$

Hypothesis 2 a, b, c: An increase in risks that are (a. malicious risks, b. tech/human failure risks, c. weather risks) will lead to an increase in discussion of that risk type (a, b, or c,) in the Senate and House budget appropriations Committee Reports.

a. $Keyword\ Malicious = B_0 + B_1\, risk + B_2\, demand\ lost + B_3\, customer\text{-}hours + B_4\, media + B_5\, House\ Majority + B_6\, Senate\ Majority + B_7\, Presidential\ Party$

b. $Keyword\ Tech\text{-}Human = B_0 + B_1\, risk + B_2\, demand\ lost + B_3\, customer\text{-}hours + B_4\, media + B_5\, House\ Majority + B_6\, Senate\ Majority + B_7\, Presidential\ Party$

c. $Keyword\ Weather = B_0 + B_1\, risk + B_2\, demand\ lost + B_3\, customer\text{-}hours + B_4\, media + B_5\, House\ Majority + B_6\, Senate\ Majority + B_7\, Presidential\ Party$

Hypothesis 3: An increase in risks impacting the grid, controlling for Congressional discussion, leads to increase in appropriations for the Office of Electricity, as a percent of total DOE fiscal year funding.

$$Funding_t = B_0 + B_1\, risk + B_2\, demand\ lost + B_3\, customers\text{-}hours + B_4\, media + B_5\, House\ Majority + B_6\, Senate\ Majority + B_7\, Presidential\ Party + B_8\, keyword\ malicious + B_9\, keyword\ tech\text{-}human + B_{10}\, keyword\ weather$$

3.6 Results

Results are presented in Table 3-3. The results of the models indicate that a one-year time lag is the appropriate lag model for all three hypotheses, indicating that this lag is be best suited for evaluating the relationship between disturbances on the grid, congressional risk perception, and federal funding for grid-related reliability, resiliency, and security improvements. Budget and appropriations proposals for fiscal year funding allocations usually take around one to two years to draft (Kocherlakota and Yi, 1996), but given the significant events and subsequent changes in DOE OE funding, as indicated above in Figure 3-5, it can be seen that policymakers can and do react more quickly depending on the circumstances. The significance of the regression models are interpreted in terms of the p-value, as is indicated in Wooldridge's discussion of time series analysis (Wooldridge, 2004, chap. 10).

Results for the first hypothesis indicate that an increase in malicious risks impacting the grid leads to an increase in the percent of Office of Electricity funding appropriations. This is the first step in a mediation hypothesis and indicates that the causal variable is associated with the outcome variable, thus allowing for the continuation of testing the next two hypotheses in the model. Results for weather-related risks and failure-relate risks are not included in the results as there is no association between these risks and subsequent federal funding.

In hypothesis 2a, the malicious disturbances on the grid (malicious risks) show a significant positive association with the discussion of malicious keywords in the Committee reports. This indicates that congressional members are aware of malicious risks impacting the grid, either through subcommittee hearings, their constituents, or

through media reports (as seen by a significant and positive association). There is a significant relationship between the political party in power and discussion of the associated keywords in the Committee Reports. Results for hypothesis 2b and 2c are not included as there is no association between tech or human-related risks nor weather-related risks and the overall outcome, federal funding, as seen in the first hypothesis.

Table 3-3. Mediation Hypothesis Model Results for Hypotheses 1, 2, and 3, time lag 1 year.

Variables	H1 (Percent of OE funding from total DOE funding)	H2a (Congressional discussion of malicious keywords)	H3 (Percent of OE funding from total DOE funding)
Risk - Malicious	0.067 ***	0.908 ***	0.067 ***
	(0.018)	(0.327)	(0.015)
Risk - Weather	-0.018	-0.287	-0.013
	(0.015)	(-0.267)	(0.012)
Demand Lost	-0.00001	-0.0001	0
	0	0	0
Customer-hours	0	-0.000003 *	0
	0	0	0
Media	0.02	1.752 ***	-0.053 ***
	(0.022)	(0.408)	(0.018)
House Majority	-0.129 ***	2.602 ***	-0.19 ***
	(0.017)	(0.302)	(0.014)
Senate Majority	0.219 ***	1.735 ***	0.135 ***
	(0.017)	(0.312)	(0.014)
Presidential Party	-0.328 ***	2.26 ***	-0.387 ***
	(0.015)	(0.268)	(0.013)
Keyword Malicious	-	-	0.025 ***
	-	-	(0.001)
Keyword Tech-Human Failure	-	-	0.001 ***
	-	-	0
Keyword Weather	-	-	0.001 ***
	-	-	0
Constant	0.92 ***	7.057 ***	0.707 ***
	(0.015)	(0.275)	(0.016)
Observations	1,011	1,011	1,011
R-Squared	0.43	0.367	0.65

Standard errors in parentheses *p<0.1; **p<0.05; ***p<0.01

Results for Hypothesis 3 indicate a significant and positive association between an increase in malicious disturbances on the grid (malicious risks) and the percent of

Office of Electricity fiscal year funding out of total DOE fiscal year funding, controlling for Congressional discussion, thus supporting the hypothesis. Due to the statistical significance between the causal variable, risks, and outcome variable, funding, this indicates a partial mediated relationship. As to be expected given the results of the second hypothesis, there is a significant and positive association between the malicious keywords and the percent of OE funding, as well as significant and positive association between the other two keyword categories as well. Media attention to disturbances appears to have a significant and negative association on the percent of OE funding.

For both Hypothesis 1 and 3, Republicans as the political party in control of the House and the Presidency leads to a significant and negative association with the percent of OE funding allocated. However a Republican-majority Senate indicates a significant positive association. Additionally for Hypothesis 2, an increase in the customers and duration impacted per year is significantly associated, and positive, with an increase in the percent of OE funding. It is unexpected that this magnitude measure, as well as the other magnitude measure, demand lost, is not significant in any of the other hypotheses.

Given the use of a time lag in these models, the number of observations that are able to be used in the analysis are 1,011 incidents out of the total 2,203 recorded incidents from the years 2000 to 2017. This is to be expected using an analysis with time lags, particularly because the disturbance database begins in 2000 but the DOE funding allocations to the Office of Electricity Delivery and Energy Reliability do not begin until 2003. Additional reduction in observations is due to the errors and variations in reporting disruptions within the OE-417 database, especially in the early 2000s compared to the more recent years. Many events did not include both a start and end time, eliminating the

possibility of calculating duration. Similarly, some events had both demand lost and customers impacted reported, while others only had one or the other (or neither). In other observations in the dataset, arbitrary units were used (such as "evening" being used to describe the start time of a disruption, or "entire facility" as a measurement for demand lost), which resulted in the elimination of those data points as well.

3.7 Discussion

The results of this analysis support the risk perception literature and the process diagram displayed in Figure 3-1. As the results for Hypotheses 1 indicate, an increase in malicious disturbances on the grid leads to an increase in Office of Electricity fiscal year budget appropriations. The results for Hypothesis 2 show an increase in malicious incidents leads to an increase in Congressional discussion about malicious risks. The results for Hypothesis 3 confirm a partial mediation, with an increase in malicious risks impacting the grid, controlling for Congressional discussion, leads to an increase in Office of Electricity funding appropriations.

The result is in line with existing risk perception literature, with information sharing and communication being a key factor in one's perception of risk (Akerlof et al., 2013; Bostrom et al., 1994; Leiserowitz, 2006; Leiserowitz and Smith, 2017). Despite so few reported physical or cyber incidents on the grid compared to weather-relate incidents, the results here suggests that the malicious risks that are reported in the media are a ultimately a topic with congressional members.

Whether the risks associated with malicious incidents are being communicated appropriately, or perhaps are being overblown to policymakers when compared to severe weather or failure risks, remains up for debate. Regardless, the results of the mediation

hypotheses model supports the final hypothesis, with policymakers viewing the risk of unnatural, man-made threats (such as physical and cyberattacks) to be of more pressing concern for funding allocations than natural occurrences (such as severe weather events), controlling for Congressional discussion. The policy response to the perceived risk of malicious attacks is measurable and positive, with an increase in the percent of Office of Electricity funding allocations being associated with an increase in malicious incidents on the grid. The policy priorities of congressional members for grid-related R&D are being address in terms of the OE funding appropriations. Risks that are inherently known to be bad or "unnatural," such as disruptions purposefully caused with the intention to cause panic, damage, or harm, are more likely to be understood as a threat (Sjoberg, 2000) and in need to of a policy response to address the issue.

The results of the mediation hypotheses model suggest a business-as-usual attitude in addressing to high number of disturbances on the grid caused by severe weather. In contrast, malicious events occur least often yet receive a measurable policy response in terms of OE funding. As reveled from the results of the first and third hypothesis, the magnitude of the disturbance incidents do not appear to influence the policymakers funding allocations to the OE. Unexpected in the results of this analysis is the lack of clarity surrounding the causes in OE funding spikes after significant events, as show in Figure 3-5. It is possible that the funding increases are a coincidence to large events, such as major Hurricanes or blackouts, but likely these single, large events are not able to be statistically linked to the funding allocations.

The results of this analysis offer a few insights regarding the funding spikes observed in the OE's fiscal year budget allocations, as seen in Figure 3-5. The large

increases in funding in the years 2006 and 2010 are associated with the grid-specific policy priorities included in the 2005 Energy Policy Act and the 2009 American Recovery and Reinvestment Act. For the 2005 EPA, these policy priorities are in part in response to the 2003 Northeast Blackout, particularly addressing the failures of the infrastructure that allowed for cascading blackouts. While the 2013 Metcalf attack has been reported to have led to an increase in grid-related funding (Parfomak, 2018; Sissine, 2015), the results from this analysis are unable to directly link the attack with the increase in funding. Instead, it appears that a combination of steadily consistent physical attacks on the grid in recent years, as well as an increase in cyberattacks targeting both the grid and other critical infrastructure sectors, can be attributed to an increase in risk perception to these threats amongst congressmembers and subsequent increases in OE funding for policy priorities concerning these issues.

Within the text of the Committee Reports, a bit more clarity is able to be gained for the differences in political party association and funding allocations. In the Report's language, it appears that the House is more blunt with their critiques of the DOE as a whole ("failures" within the Department are often cited). This may explain the negative association between malicious incidents and the percent of OE funding, suggesting a general dissatisfaction with the DOE and therefore a reluctance to provide more funding. The Senate Committee Reports, however, appears more neutral in the language used in the texts. The neutrality of the language may indicate a more open-minded approach to receiving information and communications about incidents on the grid, and therefore lead to a policy response that addresses the issues.

3.8 Conclusions & Implications for Future Research

This analysis provides a novel approach to risk perception analysis in terms of policy response. The findings support existing literature, in that communication and information sharing about risks are key to conveying risks to stakeholders and policymakers. The results go further to provide new theoretical support for perceived risks of "unnatural" threats being considered a higher priority than naturally occurring (and therefore considered uncontrollable) threats. This indicates that when national security is the issue at hand, policymakers are more likely to response with policy initiatives aimed at addressing the issues that are attributed or result from the malicious risk.

The research findings here raise multiple important next steps into determining whether risks to national security is a perceived risk that influences policymaker's budget and allocations for federal R&D funding for grid reliability, resiliency, and security. First, if policymakers are responding to incidents that threaten the electricity sector (a sector vital to national security), how large must a major incident across critical infrastructure sectors be in order to elicit a more immediate federal response? Is this dependent on media attention or another magnitude factor that has not been considered yet here: monetary costs. The Metcalf attack in 2013 caused more than $15 million in damages, but is certainly not the only malicious incident that caused a disruption to power supply and impacted customers. However, of the other attacks, Metcalf is the only one where the monetary costs of damages have been reported upon in the media (Wald, 2014). The OE-417 database does not include monetary costs of the disruptions.

This leads to a second important point: if policymakers do perceive malicious risks to the grid as a national security issue and warranting an increase in R&D allocations, albeit after a delay, why is the electricity infrastructure sector not regulated more strictly through the federal government? As it is now, the electric grid is regulated overarching through NERC but directly through local utilities, public utility commissions, regions, and states. The new NERC security improvement plans require risk assessments and audits, but no widespread minimum security standards. This leaves electricity infrastructure across the country without a minimum standard of protection. Are the areas of focus within the DOE's Office of Electricity budget allocations specifically going to address known vulnerabilities, such as those raised in Chapter 2?

Lastly, the OE-417 database is unfortunately flawed, with mismatched reporting requirements, missing data, and errors, thus eliminating many observations that could have been valuable to the analysis. However, new NERC reporting requirements have now been implemented, with a centralized database to reference (North American Electricity Reliability Corporation, 2015a). Additionally, in 2018 Secretary of Energy Rick Perry created the Office of Cyber Security, Energy Security, and Emergency Response (CESER), aimed at infrastructure protection to cyber, physical, and severe weather threats (Energy.gov, 2018). In the coming years, a beneficial next step in this research field will be to consider the new NERC reporting dataset, as well as the new CESER funding initiatives.

CHAPTER 4. WILL UPDATED ELECTRICITY INFRASTRUCTURE SECURITY PROTECT THE GRID? A CASE STUDY MODELING ELECTRICAL SUBSTATION ATTACKS

4.1 Introduction

The electricity infrastructure in the United States is not only vulnerable to weather events, technical and human errors, but also to malicious, intentional attacks (National Research Council of the National Academies, 2012). This vulnerability has been evident for decades; between 1970 and 2017, there have been approximately 527 suspected and confirmed physical attacks on grid infrastructure (Office of Electricity Delivery & Energy Reliability, 2018a). While cyberattacks are reported on less frequently and are more difficult to confirm, there have been at least 18 confirmed attacks since 2002 (Office of Electricity Delivery & Energy Reliability, 2018a). Given the vastness and age of the U.S. electricity infrastructure, it is difficult to maintain advanced security across all the sites. However, in recent years there has been more of a focus from the federal government and utility operators alike to improve physical and cyber security, with enhancements tending to start at the most vulnerable and critical sites.

One of the more publicized and costly physical attacks on the grid occurred in 2013 at the Metcalf Power Station, located in San Jose, California. This attack, which resulted in $15 million in damages and required the substation to be shut down for three weeks while initial repairs took place (Smith, 2014b), served as a catalyst for a series of attack mitigation strategies aimed at improving grid security. To prevent a similar attack from happening again, utility companies and the North American Electricity Reliability Corporation (NERC) outlined a range of security improvement measures, including more

robust physical barriers around key infrastructure, additional security technology and security personnel on site, and new risk mitigation audits to identify and communicate about vulnerabilities amongst sites (North American Electricity Reliability Corporation, 2015a).

The overarching question, to be addressed here, is how successful the security improvements proposed by utilities and NERC will be at preventing attacks. Given what is known about past attack methods and what is suspected for potential attacks, will the security improvement strategies adequately mitigate future threats? To answer this question, data and information collected from the nearly 500 past physical and cyberattacks, paying particular attention to the 2013 Metcalf attack, are used to model increasingly sophisticated attacks, including cyber-enabled physical attacks, against multiple security level scenarios. The attack scenarios are modeled in the Joint Conflict and Tactical Simulation (JCATS) software program, developed by Lawrence Livermore National Laboratory (LLNL) and used to simulate the outcomes of user-defined data (Lawrence Livermore National Laboratory, 2017).

4.2 Background

Resiliency, reliability, and security of the United States' critical infrastructure sectors, particularly the electricity and energy sector, is a focus of concern for the government, industry, and academics alike. After conducting an in-depth report in 2007 regarding electricity infrastructure vulnerabilities, the National Research Council of the National Academies pushed to have the report released to the public, so to better inform policymakers and industry experts of the report's findings (National Research Council of the National Academies, 2012). In the years since, there has been an increase in federal

research and development funding within the Department of Energy's Office of Electricity, which may indicate a renewed focus on maintaining a resilient and reliable electric grid (AAAS, 2018). Aside from industry reliability and security standards becoming more rigorous within the NERC (to be discussed in more detail in the following sections), there is a host of research focusing on risk management and disaster resiliency modeling. Past research in this area has focused on methodologies to develop baseline standards, indicators, and guides to assist in infrastructure and communities resiliency standards and risk mitigation strategies. For example, in their 2018 research, Mathias et al. outline dynamic modeling approaches to help better monitor, inform, and prepare those in charge of critical infrastructure management in the wake of threats (Mathias et al., 2018). Communication across stakeholders is often concluded to be an appropriate step in risk management and resiliency planning for natural disasters (Cutter et al., 2010; Liu et al., 2018), and is seen as a key step in NERC's infrastructure security improvements.

The simulations are based on detailed information of past attacks on the U.S. grid infrastructure. Focusing on past attacker profiles, attack methods, and subsequent damages, the model serves as a case study for a generic electrical substation attack. Given what is known about past attacks, the simulation is aimed to evaluate the potential success past attacks could have had against new security upgrades, as well as to consider what sort of damages from future, more sophisticated attacks, can be anticipated. The overarching question is whether proposed and implemented security upgrades at grid infrastructure sites can mitigate or prevent future attacks. Below, the Metcalf attack is outlined, as are the utility-level security improvements and NERC-level security

improvement recommendations that are either proposed or already implemented for electricity infrastructure across the country.

4.2.1 Metcalf Attack and Utility-Level Security Improvements

The Metcalf attack is instructive not only as a prime example of a successful, modern physical attack, but also as an illustration of the subsequent monetary damages and industry response to improving grid security. The Metcalf power station, owned and operated by Pacific Gas and Electric (PG&E) in San Jose, California, was targeted by an unknown number of attackers early in the morning on April 16, 2013. The assailants first cut underground AT&T telephone communication cables that serviced the station, and then situated themselves just out of view of the power station's security cameras. An attacker shot at the substation, including the station's transformers, with a semiautomatic rifle for just under 20 minutes. Although a security guard onsite was able to call 911 during the attack from his cell phone, and PG&E received an alert from a motion sensor triggered at the site, the attackers left the area before police arrived and have not yet been identified. The attack left 17 transformers damaged, costing PG&E $15 million in repairs and shutting down the substation for 21 days (power was rerouted to other substations in the region). The transformers were damaged and not destroyed, leading to debate within the industry and the Federal Bureau of Investigation (FBI) about whether the attackers specifically targeted the transformers or were shooting randomly (Smith, 2014a). Transformers cost approximately $3 million each, so targeting transformers has the potential to result in a costly attack (Office of Electricity Delivery & Energy Reliability, 2012).

Perhaps because this attack could have resulted in extremely high repair costs, or perhaps because the attack demonstrated a vulnerability at electricity infrastructure across the U.S., PG&E and other utility operators took notice and initiated security improvements. In December of 2014, PG&E pledged $10 million over three years to improve their critical infrastructure protection for power and substations similar to Metcalf. After being fined $50,000 by the State of California for the theft of $40,000 worth of construction equipment from the Metcalf site, PG&E declared in 2015 an additional $200 million investment for substation security at the most critical and/or most vulnerable facilities across California. Approximately 40 percent of the investment is dedicated for physical barrier security and 60 percent will go towards technological security improvements (California Public Utilities Commission, 2015).

Some of the initial security improvements PG&E focused on are round-the-clock security guards on site (plus additional training for overnight guards) (California Public Utilities Commission, 2015), removing foliage and undergrowth that could provide hiding places, improving and increasing lighting onsite, and adding security perimeter and internal fencing (chain link and concrete) (Pacific Gas and Electric, 2014). Additional and improved security camera technologies (such as thermal cameras and enhanced detection analytics) are proposed to be added, as well as a gunshot detection system (California Public Utilities Commission, 2015). Other utilities across the country are following suit. Despite not experiencing any publicized attacks on their infrastructure, Virginia Dominion Resources pledged to invest $300 to $500 million in 2014 to improve security at their sites (Smith, 2014a).

4.2.2 NERC-Level Security Improvements

More overarching, however, are the measures NERC has taken to increase security vulnerabilities, awareness, and information sharing across the NERC regions. First, in January of 2015, the Electric Information Sharing and Analysis Center (E-ISAC) within NERC created the Physical Security Analysis Team (PSAT). The PSAT's mission is to assist NERC members in identifying vulnerable physical security infrastructure and develop new physical security plans. Members receive physical security updates and suggestion bulletins, information, and planning scenario pamphlets. For example, bulletins have focused on unmanned aircraft surveillance systems at vulnerable infrastructure, and planning exercises have outlined worst-case scenarios (North American Electricity Reliability Corporation, 2016). In March of 2015, the Physical Security Advisory Group (PSAG) was created to assist in analyzing current and potential physical security threats. Members of PSAG consist of industry experts and representatives from both the Department of Energy and the Department of Homeland Security (North American Electricity Reliability Corporation, 2016). NERC views membership participation and communication within the E-ISAC portal to be a critical component in both physical and cyber security improvements (awareness, troubleshooting, security mitigation efforts). One of the main goals is to have physical and cyber security data and standardization metrics available from a centralized source so all members have access to the same information and incidents are easily shared (North American Electricity Reliability Corporation, 2016). NERC's emphasis on communication and information sharing is in line with other research relating to critical

infrastructure risk management and disaster resiliency as well (Liu et al., 2018; Mathias et al., 2018).

The main NERC contribution to improving electricity infrastructure security is the CIP-014-2 standards, requested by the Federal Energy Regulatory Commission (FERC) in March of 2014 and finalized in 2015 (North American Electricity Reliability Corporation, 2015a, 2014). The purpose of CIP-014-2 is to protect vulnerable and critical transmission stations and substations from becoming inoperable, damaged, or resulting in a cascading failure as a result of a physical attack (North American Electricity Reliability Corporation, 2015b). This applies to substations 500 kilovolt (kV) or higher and certain substations between 200 kV and 499 kV that are deemed high priority or critical (North American Electricity Reliability Corporation, 2015a). NERC outlines six requirements within the CIP-014-2 plan:

1. Owners of transmission stations must provide risk assessments to current and future infrastructure.
2. A third party must verify the risk assessment and provide recommendations for risk mitigation.
3. The risk analysis must then be provided to the managers or operators of said infrastructure.
4. For all of the sites where risk assessments were performed, the owners must then also provide an evaluation and identify vulnerabilities of potential physical attacks.
5. All owners must provide a detailed physical security plan to have on file after the risk assessment is conducted.
    a. The plans should include: identifying vulnerabilities; outline deterrent and mitigation plans of potential attacks; communication plans, detection techniques; how to contact and coordinate with law enforcement in the event of an attack; provide a timeline of when physical security

improvements will be initiated and completed; how to continuously monitor and update security plans given evolving physical threats.

6. A third party should then review the physical security evaluation and resulting plan that is developed. The third party must be certified to conduct physical protection assessments, be from a NERC-approved organization, or be a government agency, law enforcement, or military security expert.

4.3 Data and Methodology

For this analysis, a substation operating as part of the U.S. electrical grid is created as the site for which all security upgrades are implemented and all attacks take place. Though the substation is fictional and generic, its layout, equipment placement, surrounding environment, and other features are similar to those found at substations in the U.S. The fictional substation is located on the outskirts of a metropolitan area, surrounded by vegetation and with a main road nearby. Each scenario in the analysis occurs at twilight. The targets are the 20 transformers onsite. Transformers are targeted due to their critical role in the delivery of reliable electricity, the fact that they are expensive and difficult to repair and replace, and because they have been targeted frequently in the past (including the 2013 Metcalf attack) (National Research Council, 2012).

4.3.1 JCATS MODELING

To model the incremental security upgrades against different attack scenarios, the computer modeling program JCATS is used. JCATS is a program created and maintained by Lawrence Livermore National Laboratory, used to stochastically determine the outcomes of discrete events and actions, with the statistical data to run the scenarios defined by the user (Lawrence Livermore National Laboratory, 2017). The first steps in

building a model in JCATS is to define the problem, conditions, target types one wishes to model, as well as the defensive and adversary forces. Next, the aims of the attack and tactical information of both the adversary and the defenders are inputted. In building the specific scenarios of the model, details about the terrain, actor behaviors, and tactical information are determined by the user (Conflict Simulation Laboratory, 2018a, 2018b).

While much of the data that is input into JCATS is collected by the user (here, information about past physical and cyberattacks on electricity infrastructure), there are some parameters pre-programmed within the computer software. For example, military field experiments provide specific data outputs for weapon range, visibility, and probability line of sight acquisitions in various lighting and vegetation conditions. Previous research has used JCATS primarily for military-related research, including emergency management and response modeling (Kincaid et al., 2003), wargames training to simulate possible outcomes for military troops in various terrain conditions (Bowers and Prochnow, 2003), and to provide a risk assessment for potential damages to U.S. ports from maritime improvised explosive devices (Paulo et al., 2010). The ability for the JCATS computer program to create specific terrain, infrastructure, and conditions allows for users to input the conditions for a disaster, emergency, or attack, including behavior of the actors, weapons, and safety procedures.

In this study, there are two categories of user-defined data: security upgrade levels and attacker profiles. Security upgrade levels include the baseline security standards currently used at most substations through to the most stringent security standards currently being implemented by utilities. The attacker profiles are three distinct groups of adversaries, ranging from Amateur to Elite, that attack the substation in the model. The

data collected and assumptions used to create the user-defined security upgrade levels and attacker profiles are explained below, preceded by description of the site and its environment that is used throughout the simulations.

4.3.2 Security Upgrade Levels

The security upgrade levels are designed to indicate the physical security improvements to critical grid infrastructure that have been proposed or implemented by grid operators, NERC, or federal and state governments (as described in the previous section). Starting with basic physical security features that most substations already have (noted as "Baseline" in the analysis), four incremental security upgrades ("Security Upgrade 1-4") scenarios show increasingly robust security at the model's substation. A summary of the Baseline and Security Upgrades 1-4 can be seen in Table 4-1.

Physical security improvements start with the lighting at the substation and the vegetation surrounding the substation. As noted in the previous section, utilities aim to improve the ability of security cameras and guards to spot potential intruders and threats by increasing the light levels and reducing foliage (Pacific Gas and Electric, 2014). The JCATS data that reflects the ability of an attacker to identify and attack a target through different light levels is collected by the U.S. Army Materiel Systems Analysis Activity (AMSAA). Through field experiments, the AMSAA collects acquisition of target and performance data "based on the ACQUIRE type sensor performance and technical data," meaning the troop's ability to acquire and strike a given target in various lighting levels.[2]

[2] AMSAA Special Publication No. SP-97, The Compendium Of Close Combat Tactical Trainer Algorithms, Data, Data Structures And Generic System Mappings.
ACQUIRE-TTPM Implementation Guide for Combat Simulations 21 July 2008
Distribution is authorized to U.S. Government Agencies and their contractors: Other requests shall be referred to Director, U.S. Army Materiel Systems Analysis Activity, APG, MD 21005-5071

While the time of day is "twilight" during all scenarios in the model, lighting at the substation improves from "low" (twilight with shadows) in the Baseline to "extra high" (overcast sunlight) in Security Upgrade 4.

Table 4-1. Security Upgrade Scenarios (laboratory-specific reference number LLNL-TR-746040).

	Baseline	**Security Upgrade 1**	**Security Upgrade 2**	**Security Upgrade 3**	**Security Upgrade 4**
Time of day	Twilight	Twilight	Twilight	Twilight	Twilight
Lighting	Low (Deep Twilight)	Medium (Twilight)	Medium (Twilight)	High (Heavy Overcast)	Extra High (Overcast Sunlight)
Vegetation	High (0.6 probability line of site blocked (PLOSB)	Medium (0.2 (PLOSB)	Medium (0.2 (PLOSB)	Low (0.05 (PLOSB)	Low (0.05 (PLOSB)
Perimeter Details	Chain fence	Chain fence + interior chain fence	Chain fence + interior chain fence	Concrete wall + internal chain fence	Concrete wall + internal chain fence + armored shielding around transformers
Cameras / Motion Sensors	Basic (70% probability of detecting intruder)	Additional Cameras / Sensors (80% probability of detection)	Additional Cameras / Sensors (80% probability of detection)	Advanced cameras + motion sensors weaved into fencing (90% probability of detection)	SU3 features + gunshot detection sensors (100% probability of detection)
Security Presence / Engagement	Two. No patrol, no engagement	Two. No patrol, no engagement	Two, with one patrolling on foot. No engagement	Two, with one patrolling on foot. No engagement	Two, with one patrolling in a vehicle. Engagement
Police Engagement	Yes	Yes	Yes	Yes	Yes

Field experiments determine the probabilistic attenuation for line-of-sight, meaning "the probability of acquiring a target in (or through) a feature depends on how far into (or through) the feature an observer has to look." The model assumes that the substation is surrounded by vegetation, and security improvements reduce the probability line-of-site blocked (PLOSB) from "high" (0.6 PLOSB) in the Baseline to "low" (0.05

PLOSB) in Security Upgrades 3 and 4 (assuming there will always be a tree or boulder in the area, modeled vegetation is never reduced to 0 PLOSB).

Additional security features include physically securing the perimeter, securing the transformers, and improving and/or increasing the range of security cameras, motion sensors, and gunshot detection sensors. In the Baseline scenario, the substation is surrounded by a single chain-link fence. As security improvements increase incrementally, additional chain-link fences or concrete walls are erected (Security Upgrades 1-3) with the goal of armored shielding around the transformers (Security Upgrade 4). For security cameras, motion sensors, and gunshot detection sensors, probability of detection is used as an indicator to measure the technological improvements, increase in number, and increase in range of the equipment. However, it must be noted that cameras in areas with relatively high traffic (cars, pedestrians, wildlife) tend to only focus at the immediate 10-foot range surrounding the exterior fence around the site, and motion sensors will only react when disrupted.[3] In the Baseline, cameras and motion sensors have a 70% probability of detecting an intruder, increasing to 90% in Security Upgrade 3. In Security Upgrade 4, probability of detection is increased to 100% due to the addition of gunshot detection sensors, which are assumed to be one of the higher tiers of physical security upgrades a utility may implement.

Responding security and police are included in the security upgrade scenarios. Based on knowledge of existing electrical substation security and the intended security improvements, it is assumed that there will always be two security guards onsite. At the Baseline and in Security Upgrade 1, both security guards remain the security booth. In

[3] Based on discussion with Military experts at LLNL

Security Upgrade 2 and 3, one security guard is patrolling on foot, increasing the time the guard can detect and report an attack. In Security Upgrade 4, a guard is patrolling in a vehicle, further increasing the detection and reporting time. Only in Security Upgrade 4 do the responding guards engage with the attackers.

4.4 Attacker Profiles

Three distinct attacker profiles are created to demonstrate the varying extent of damages that can be inflected upon grid infrastructure depending on the training and determination of the assailants. These three attacker profiles are Amateur, Trained, and Elite. The distinction between the three profiles is based on examples and knowledge gained from past grid attacks. Incidents of sabotage without planning or an understanding of how the targeted infrastructure operates are classified as Amateur incidents. For example, incidents in which the assailant has manually tried to unscrew bolts of electricity poles or pylons are considered Amateur attacks (James, 1981). Attacks demonstrating knowledge of the infrastructure and/or methods used to carry out the attack are classified as Trained incidents, such as when a former electrical engineer used thermite to attempt to burn through high voltage power lines (Rosen, 2016). While there has yet to be an Elite attack on the grid, an Elite assailant is considered someone who has been specifically trained to a high standard in both the attack method and the infrastructure operations, components, and weaknesses.

As stated, the JCATS program requires users to input some information and data into the system to create statistical simulations. For the attacker profiles, details about weapon types (semiautomatic rifles modeled after those used in the Metcalf, and basic improvised explosive devices) already existed in the JCATS database. The probability

that the attackers hit their target, and the probability that said hit causes damage or destroys the target, is user input. For this model, these probabilities were determined first by using the Metcalf attack as a baseline case study. As mentioned above, given the differing opinions between FBI investigators and industry experts for whether the Metcalf attack was carried out by amateurs or perpetrators with more training (Smith, 2014a), the hypothesis in this study is that amateur attackers in the model will damager fewer than the 17 transformers damaged in the actual Metcalf attack, whereas trained attacks in the model will damage more than 17. To fine-tune this hypothesis, military experts at LLNL were consulted. These military experts provided information about hit accuracy, expected damage due to weapon type, and the variations between the attacker profiles compared to police and security forces.[4] Lastly, the probability estimates in Table 4-2 were cross referenced with literature discussion of police and security target accuracy, where the estimates were confirmed (Lewinski et al., 2015).

Additionally, the military experts provided insight about attacker movements, plans, and interactions with responding security and police forces. [5] Based on these conversations, as well as information about past physical attacks on the grid as presented in Chapter 2, it is assumed that the goal for Amateur and Trained attackers is to cause as much damage as possible to the infrastructure only. Therefore, in the model simulations, Amateur and Trained attackers flee the scene when security or police respond to the attack. Elite attackers, however, are assumed to be highly trained by a sophisticated group or nation state and to be willing to engage with responding security or police forces in

[4] Lawrence Livermore National Laboratory, Global Security Program, personal communication, January 30-February 1, 2018.
[5] Lawrence Livermore National Laboratory, Global Security Program, personal communication, January 30-February 1, 2018.

order to continue their planned attack. In the model, onsite security forces do not engage unless shot at first: the LLNL military experts advised that proper protocol for security is to call the local police or SWAT team.[6] Amateur and Trained attackers flee when onsite security arrives, but Elite attackers confront responding security officers. The responding off-site police forces do engage with the attackers, meaning the model only shows security and police engagement with the Elite attackers.

Table 4-2. Attacker Profiles, LLNL-TR-746040.

Attacker Profiles			
	Amateur	**Trained**	**Elite**
Probability of Hit	85%	96%	100%
Probability of Damage: None	27.5%	23.5%	20%
Probability of Damage: Damaged	72%	74.5%	77%
Probability of Damage: Destroyed	0.5%	2%	3%
Engagement with Security/Police	None	None	Yes
Weapon Details	AK47 7.62x39, 150 rounds each, 500 meter range	AK47 7.62x39, 150 rounds each, 500 meter range	AK47 7.62x39, 150 rounds each, 500 meter range
Explosives Details	None	None	Generic IEDs, set off with timer, 10m explosive range. Probability: 80% damage, 20% kill
Breach Perimeter	No	No	Yes (1 minute to cut fence, 2 minutes to climb barrier)
Additional Equipment	None	None	Equipment to breach perimeters; Night vision/thermal goggles

4.5 Attack Scenarios

Given the differences between each security upgrade level and the three attacker profiles, there are differences in how each attack scenario in the model plays out. The

[6] Lawrence Livermore National Laboratory, Global Security Program, personal communication, January 30-February 1, 2018.

main differences are outlined below in Table 4-3. In the Baseline and Security Upgrade 1, the terrain is perfectly flat. Therefore, once a wall is constructed in Security upgrade 3, all attacks would be thwarted due to the attackers being unable to acquire a line of sight to the target. However, it is unlikely that all terrain will be absent of trees, hills, boulders, or other features that one could climb to get a better view of the targets. As such, a 1.5-meter hill is added to the terrain in Security Upgrades 3 and 4. This hill represents terrain features (naturally occurring features in the environment or even just standing on top of a vehicle) that could allow for assailants to continue their attacks despite a concrete wall blocking an eye-level line of site.

The next set of details that varies for the attack scenarios is how the assailants act. The Amateur and Trained attackers never breach the perimeter of the substation during any attack scenario, therefore they never trigger security cameras. This is because for a substation such as this, situated just outside of a metropolitan area, the activity and traffic nearby is enough to require that cameras only be situated to cover ten feet outside the exterior fence; otherwise passing cars, pedestrians, and animals may constantly trigger the camera's activity alerts.[7] The motion sensors will eventually be triggered in each Security Upgrade scenario for the Amateur and Trained attackers, as some of the shots fired will hit the exterior fencing (where motion sensors are located),[8] such as was the situation during the Metcalf substation attack. While security guards are in the guard booth onsite in the Baseline and Security Upgrade 1 scenarios, in the final Security

[7] Lawrence Livermore National Laboratory, Global Security Program, personal communication, January 30-February 1, 2018.
[8] Lawrence Livermore National Laboratory, Global Security Program, personal communication, January 30-February 1, 2018.

Upgrade (Level 4), gunshot detection sensors are installed, meaning that security guards onsite are alerted to an attack even quicker.

Table 4-3. Attack Scenario Details.

<table>
<tr><td></td><td colspan="6">Attack Scenario Details</td></tr>
<tr><td></td><td></td><td>Baseline</td><td>Security Upgrade 1</td><td>Security Upgrade 2</td><td>Security Upgrade 3</td><td>Security Upgrade 4</td></tr>
<tr><td rowspan="4">Attacker Profile:</td><td>Amateur</td><td colspan="2" rowspan="2">Never breaching perimeter, so never triggering cameras, eventually gun shots will trigger motion sensors.</td><td colspan="2" rowspan="2">Foot patrolling security guard lead to quicker reaction time in SU2-3</td><td rowspan="2">Gunshot detection sensors triggered. Guard patrolling in vehicle.</td></tr>
<tr><td>Trained</td></tr>
<tr><td>Elite</td><td colspan="4">One attacker is always breaching perimeter to place IEDs, so always triggering cameras/motion sensors based on probability of detection (listed in Table 4-1)</td></tr>
<tr><td></td><td colspan="2">-</td><td colspan="2">Foot patrolling security guard lead to quicker reaction time in SU2-3</td><td>Guard patrolling in vehicle.</td></tr>
<tr><td rowspan="3">Response Time:</td><td>Security</td><td>Recognize: 5 mins
React: 5 mins</td><td>Recognize: 5 mins
React: 5 mins</td><td>Recognize: 1 mins
React: 1 mins</td><td>Recognize: 1 mins
React: 1 mins</td><td>Recognize: 0.5 mins
React: 0.5 mins
Arrive: 2 mins</td></tr>
<tr><td>Police</td><td colspan="5">Travel time to arrive at the substation is always 10 mins</td></tr>
<tr><td>Additional Notes</td><td colspan="3">Flat terrain</td><td colspan="2">1.5 meter hill added to environment to demonstrate terrain variability</td></tr>
</table>

Last, the time it takes for security and for police to respond to the threat varies for each Security Upgrade. Three factors contribute to the response time: the time it takes for onsite security to recognize that an attack is taking place (based on cameras, sensors, or hearing or seeing an attack themselves), the time it takes the onsite security to react (identifying the location of the attack, the nature of the attack, notifying off-site police), and the time it takes for off-site police (or SWAT) forces to arrive. It is assumed that once onsite security places the call for police response, the time to travel to the substation will always take 10 minutes, regardless of security upgrade level. As mentioned previously, the Amateur and Trained attackers do not engage with security or police

forces, but Elite attackers do. Therefore, in Security Upgrade 4, the onsite security guard patrolling in a vehicle responds to the situation unfolding and upon arrival to the scene, engages with the attacker who breached the perimeter to place improvised explosive devices (IED).

4.6 Results

4.6.1 Physical Attacks

Each Security Level Upgrade scenario is run against the three attacker profiles in "batches," meaning JCATS cycles through each scenario 100 times each in order to produce a statistical probability of the outcomes. The baseline substation model in JCATS is shown in Figure 4-1 (with the attackers red, security blue, and police vehicle blue) and the results are displayed below in

Table 4-4 and Figure 4-2. The outcomes of interest are the expected average number of "targets" damaged or destroyed by firearms and IEDs in each scenario. For all scenarios, the first target assessed is the average number of transformers (out of 20 total on site) damaged and destroyed in each attack scenario. For the Elite attacker attack scenarios, the average number of transformers damaged and destroyed by the three IEDs placed onsite is also recorded. As discussed previously, the Amateur and Trained attackers flee the scene once onsite security or offsite police arrive to the scene of the attack, therefore there is never any engagement between the two groups. However, the Elite attackers do engage with responding security and police, with the attackers always shooting first. This engagement means that Elite attackers, security guards, and police officers are also "targets" assessed as damaged or destroyed in the model within the Elite Attacker scenarios.

Figure 4-1. Baseline Model of Substation in JCATS, LLNL-PRES-746039.

Using the 2013 Metcalf attack and information about other past physical attacks on electricity infrastructure as a guide, the Baseline Security Level Upgrade scenario performs in the expected range of damaged and destroyed transformers. While the Metcalf attack resulted in 17 damaged transformers, the Amateur attackers perform less successfully, with 15 transformers damaged and fewer than one transformer destroyed, on average. The Trained attackers fair better, with nearly 15 transformers damaged and at least four destroyed, on average, indicating that those trained more extensively with the attack weapons will have a better chance of destroying the target. The Elite attackers damaged and destroyed transformers with both firearms and IEDs, but the total count throughout all security upgrade scenarios is not exceedingly high due to one Elite member spending time breaching the perimeter and placing the explosives before beginning to fire upon the substation. There is no engagement between security or police

in the Baseline because the guards stay in their booth and the attack concludes before the responding officers arrive.

In the subsequent Security Level Upgrades, vegetation is reduced and lighting increases, as do cameras and sensors. In Security Upgrade 1, interior chain link fences are added around the transformer area, in addition to the perimeter chain fence. This reduces the line of site for the attackers to acquire the targeted transformers, reducing the average number of transformers damaged and destroyed by all three attacker profiles. Furthermore, even though the response time does not change from the Baseline, the additional chain fence that the Elite attacker must cut through to place the IEDs means that the attack is slowed enough to the point where there is engagement between the Elite attacker and the responding police forces. The Elite attacker is destroyed (i.e. “killed”) almost 100 percent (0.99) of the time during the attack scenario.

Security Upgrade 2 proceeds similarly, with the only upgrade in security from Level 1 to 2 being that there is a security guard patrolling on foot. The patrolling officer is able to reduce the amount of time it takes to recognize that an attack is taking place and react appropriately by calling in for police response. However, the patrolling guards in the models have randomized patrol routes, and in this scenario the route occasionally means the guard is close enough to be targeted by Elite attackers. In running this scenario, the guard is damaged (i.e. “injured”) 26 percent of the time and destroyed (i.e. “killed) 43 percent of the time.

Table 4-4. Physical Attack Scenario Results, LLNL-TR-746040.

Security Level	Attacker Profile	Target	Damaged by Firearms	Destroyed by Firearms	Damaged by IEDs	Destroyed by IEDs
Baseline	Amateur	Transformer	15.46	0.93	-	-
	Trained	Transformer	14.9	4.4	-	-
	Elite	Transformer	10.86	3.67	2.52	0.48
		Elite Attackers	0	0	0	0
		Security Guards	0	0	0	0
		Police	0	0	0	0
Security Upgrade 1	Amateur	Transformer	10.54	0.99	-	-
	Trained	Transformer	8.07	3.78	-	-
	Elite	Transformer	7.97	3.4	2.32	0.68
		Elite Attackers	0	0.99	0	0
		Security Guards	0	0	0	0
		Police	0	0	0	0
Security Upgrade 2	Amateur	Transformer	10.86	0.74	-	-
	Trained	Transformer	7.82	4.03	-	-
	Elite	Transformer	7.77	3.6	2.35	0.65
		Elite Attackers	0	0	0	0
		Security Guards	0.26	0.43	0	0
		Police	0	0	0	0
Security Upgrade 3	Amateur	Transformer	15.97	0.79	-	-
	Trained	Transformer	9.94	4.3	-	-
	Elite	Transformer	9.37	4.31	2.35	0.65
		Elite Attackers	0	0	0	0
		Security Guards	0.37	0.4	0	0
		Police	0	0	0	0
Security Upgrade 4	Amateur	Transformer	0.71	0	-	-
	Trained	Transformer	5.13	0.14	-	-
	Elite	Transformer	2.61	0.08	1.11	0.23
		Elite Attackers	0.13	1.18	0	0
		Security Guards	0	0	0	0
		Police	0	0	0	0

In Security Upgrade 3, reduction in foliage, increase in lighting, and increase in the number and technological advancement of the cameras and sensors continue to

improve. Additionally, a concrete barrier is constructed around the perimeter of the site, in addition to the exterior chain fencing and interior chain fencing. With these security improvements, simulation showed that if the terrain were perfectly flat, each group of attackers would be unable to acquire the targets and all future attacks would be thwarted. Given this development, further interviews were conducted with the military experts at LLNL. They advised that it would be very unlikely that the terrain would be devoid of trees, hills, boulders, or the ability to bring in a vehicle or other device to stand on for greater visibility range. The experts agreed that a flat terrain would not deter attackers and the mission would still be carried out across the various attacker skill levels.[9] Therefore, a 1.5-meter hill was added to the simulations for the Security Upgrade 3 and 4 scenarios. As such, all three attackers improve in the total number of transformers damaged and destroyed on average. As in Security Upgrade 2, an unfortunate patrol route for the security guard results in engagement between the Elite attacker and the guard. The guard is injured 37 percent of the time and killed 40 percent of the time.

In Security Upgrade 4, the most extensive security improvements are implemented. In addition to the incremental foliage reduction, lighting increase, and camera and sensor numbers increasing and technology improvements, gunshot detection sensors and armored shielding around each transformer are added. The shielding reduces the line of sight for the attackers, meaning that acquiring the targets is more difficult. For the Elite attackers, the assailant breaching the perimeter is able to climb the concrete barrier but not get around the armored shielding. The IEDs placed at the bases of the

[9] Lawrence Livermore National Laboratory, Global Security Program, personal communication, January 30-February 1, 2018.

transformers only damage 1.1 transformer on average, and destroys one in less than a quarter of the simulated attacks.

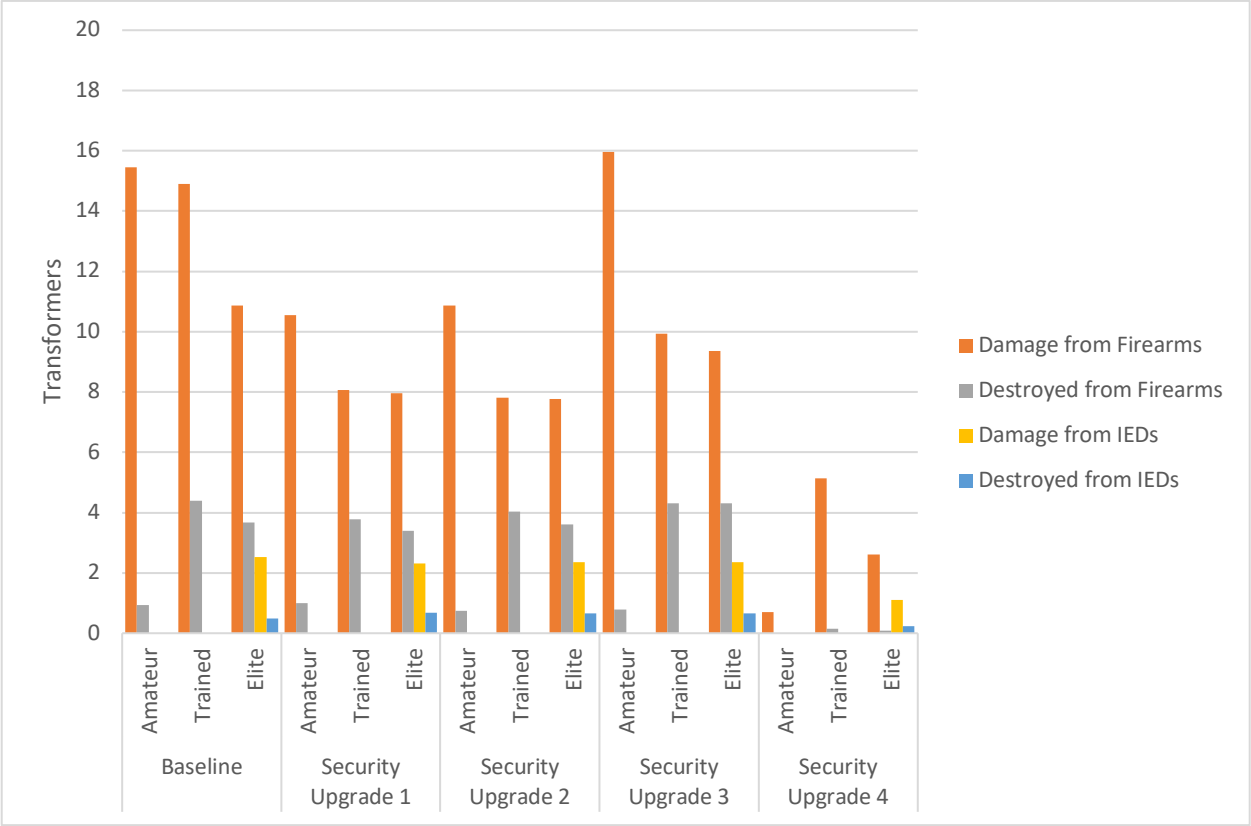

Figure 4-2. Damaged or Destroyed Transformers from a physical attack, based on Security Upgrade Level

The improvements in technology, such as the gunshot detection sensors, improve the attack recognition and guard reaction time, leading to a quicker police response. As such, the Elite attackers are thwarted, with both the patrolling security guard and responding police arriving to the scene while the attack is still occurring. Because both Elite attackers are within range of responding officers, rather than just one, interpreting the results of injuries and death is slightly different for this scenario. On average, 0.13 out of the two Elite attackers are injured during each of the 100 runs, meaning 6.5 percent of the attackers are injured. Conversely, 1.18 Elite attackers are killed on average during the attack scenario, that in total over 100 runs, 59 percent of the time the attackers are killed.

4.6.2 Cyber-Enabled Physical Attacks

The modeled attack scenarios are all physical attacks. Data on suspected and confirmed attacks show that physical attacks remain a continuous threat against electricity infrastructure, but the data also indicate that cyberattacks are a rising threat (Office of Electricity Delivery & Energy Reliability, 2018a). There has been a rise in lone wolf attacks across critical infrastructure, and cyberattacks may be particularly appealing in that little to no group organization is required to carry out an attack (Ellis, 2014). Furthermore, cyberattacks may offer a sense of security and decreased personal risk, since the orchestrator can conduct the attack remotely.

To assess cyberattack risks, two additional attack scenarios are implemented, each being a cyber-enabled physical attack. A cyber-enabled physical attack is a physical attack in which security features at a site are tampered with remotely (a cyberattack) to assist the onsite attack. In these two attack scenarios, the highest level of security in the model, Security Upgrade Level 4, is attacked first through cyber methods and then by the Trained and the Elite attackers. Prior to the physical attack, the communication lines, security cameras, motion and gunshot detection sensors, and lighting are all disabled through cyber means. It is assumed that Trained and Elite assailants have basic thermal night vision goggles. The physical attacks commence as in the previous scenarios, with the Trained attackers firing from the field and the Elite attackers both firing and breaching the perimeter to place IEDs. Cut communication lines, coupled with the inability to quickly detect the direction of the attack, results in security taking up to one minute to recognize an attack is taking place (a patrolling vehicle guard helps keep this time low) and an additional one-minute delay to react to the attack (the delay stemming

from the need to bypass normal radio communications and use cellphones to report an attack instead). Responding police officers take the expected 10 minutes to arrive on site.

Table 4-5. Security Upgrade 4: Cyber-Enabled Attack

		Target	Damage from Firearms	Destroyed from Firearms	Damage from IEDs	Destroyed from IEDs
Security Upgrade 4: Cyber-Enabled Attack	**Trained**	Transformer	5.81	0.21	-	-
	Elite	Transformer	1.81	0.07	1.47	0.42
		Elite Attackers	0.12	1.86	0	0
		Security Guard	0	0	0	0
		Police	0	0	0	0

The results of these cyber-enabled physical attacks, as shown in Table 4-5 and displayed in Figure 4-3, indicate that the most advanced security improvements continue to help mitigate the damage that could be inflicted from an attack. While, on average, 5.8 transformers are damaged during the Trained attack, fewer than one transformer is destroyed. In the Elite cyber-enabled physical attack, only 1.8 transformers are damaged from firearms and 1.5 damaged from the IEDs, on average. Fewer than one transformer on average is destroyed via either method of attack. Additionally, despite the communication lines being down, which increases response time, the time it takes the Elite attacker to cut through and climb over the barriers to get into the substation is still enough to result in an encounter with responding police officers. As such, out of 100 runs with two Elite attackers, the attackers are injured 6 percent of the time and killed 93

percent of the time, on average. Figure 4-4 shows an interaction between security and the Elite Attackers during the cyber-enabled attack in the JCATS simulation.

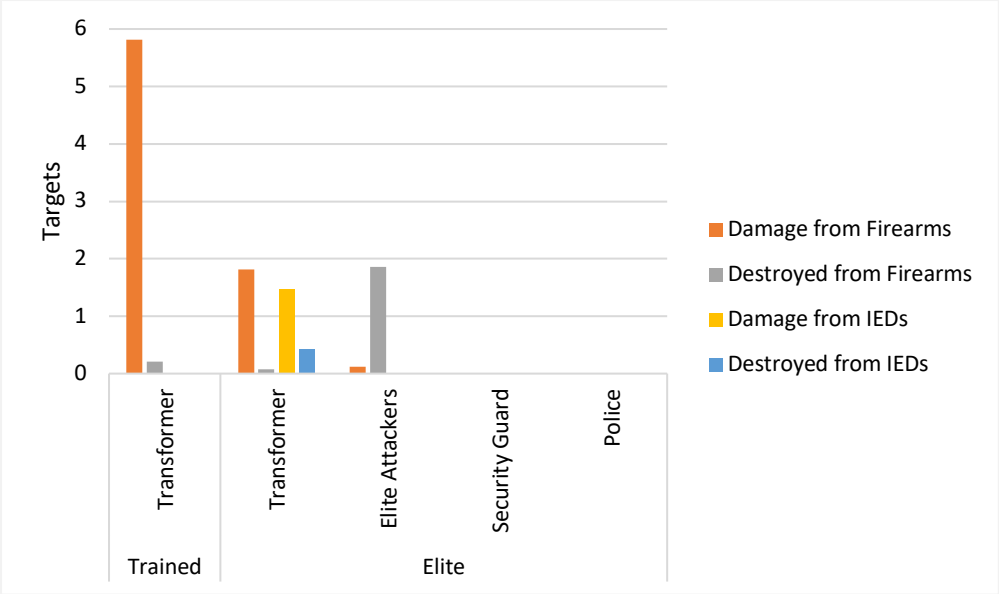

Figure 4-3. Damaged or Destroyed Targets in Cyber-Enabled Physical Attacks

4.7 Discussion

The results of the simulations indicate that for a general substation, such as the one described here, incremental security improvements can mitigate the effects of a physical attack. Clearing vegetation and increasing the amount of light at a site can help the guards detect an attack quickly and reduce hiding places for would-be attackers. However, the improved visibility also helps attackers have an improved line of site and a higher probability of acquiring the targets. Security cameras have limited effect in thwarting physical attacks, as assailants with firearms can remain outside the range of detection of the cameras and still acquire the targets inside. An increase in the amount of motion sensors woven into or placed on the fencing and external barriers can help make up for this, by detecting shots and the direction of attack earlier on. Patrolling guards

increase the response time to confront the attackers, thus potentially ending the attack before the maximum amount of damage can be inflicted on the equipment.

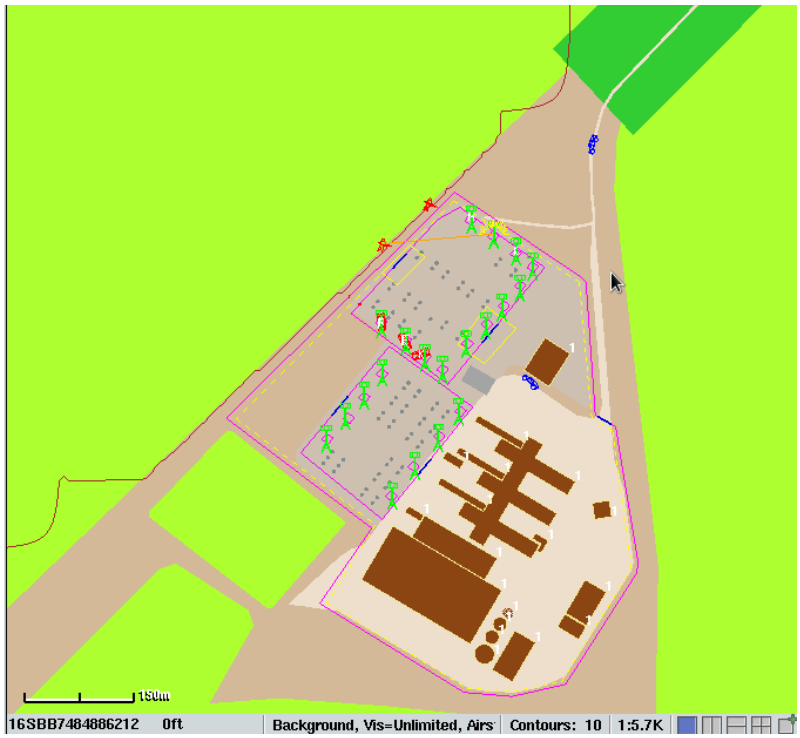

Figure 4-4. Elite Attackers (red) in a Cyber-Enabled Physical Attack, LLNL-PRES-746039

The results of the incremental security upgrade levels, as seen in Figure 4-2 show the greatest improvements to security come from better barriers around the substation (comparing Security Upgrade 1 to 2) and especially around the transformers themselves (comparing Security Upgrade 3 to 4). Transformers damaged or destroyed by both firearms and IEDs across the range of attacker profiles drops when these additional physical barriers are added to the sites. Even when terrain is not perfectly flat, a feature added in Security Upgrade 3 that exposes the transformers significantly, armored shielding results in the most significant drop in damaged and destroyed transformers.

A notable takeaway from both the initial physical attack scenarios and the cyber-enabled physical attack scenarios is that IEDs are not a very effective method of attack.

Firearms, especially coordinated firearm attacks, inflict the most damage on transformers. While areal drone technology is becoming easier to access, delivering IEDs via drones would likely still be less effective than a firearm attack due to drone weight limitations. Even if the trained or elite attackers had access to high-end heavy-payload drones that can carry up to 20 pounds (Brouillette, 2017), military experiments conclude that a solider can carry approximately 75 pounds of additional weight.[10] Generic IEDs typically weigh between 10-15 pounds,[11] meaning a single attacker could carry approximately five to seven IEDs while a drone could only carry one to two IEDs. Therefore, while the preventive measures being proposed by utility companies and NERC are useful in mitigating damage from attacks both outside and inside the perimeter of the substation, perhaps further consideration is needed in how to reduce the vulnerability of substations from firearm attacks.

Clearing vegetation and increasing lighting at infrastructure sites is helpful, but a motivated individual, trained to use a firearm, can still implement a fairly damaging attack from outside the security camera's view. Fencing and walls around the perimeter of the sites and internally around key infrastructure, such as transformers, helps reduce the line of sight for would be attackers, though this varies depending on an attacker's ability to secure a better vantage point, such as a naturally occurring higher elevation (a few meters) or brining in outside structures to position themselves on top of. As demonstrated in the security upgrade levels, armored shielding appears to be the

[10] Lawrence Livermore National Laboratory, Global Security Program, personal communication, January 30-February 1, 2018.
[11] Lawrence Livermore National Laboratory, Global Security Program, personal communication, January 30-February 1, 2018.

preventative measure best equipped to reduce an attacker's line of sight acquisition of a target from both high and low elevation vantage points.

As mentioned previously, JCATS is used primarily to offer feasible predictions of future attack, wargame simulations, emergency scenarios, or to validate outcomes of past attacks. In this model, the 2013 Metcalf attack is used as a baseline and the model scenarios are validated in that amateur attacks are less successful at damaging or destroying transformers than the actual Metcalf attackers, whereas trained attackers are more successful. However, for the sake of consistency, the model presented in this research kept many parameters consistent across attacker profiles, such as weapon type. It is plausible that the more skilled attackers may choose a different weapon type, thus impacting the ammunition capacity, weapon's range, and target accuracy capabilities. Variations such as this would likely alter the specific numbers of damaged or destroyed targets in the results, but not the overarching results indicating that the more skilled an attacker is, the more damage they can inflict upon a target. Additional variations to the model to be considered in future iterations of attack scenarios include alterations to attacker behavior. For example, the Elite attacker's behavior could be programed instead for both perpetrators to fire their weapons at the transformers, rather than one perpetrator breaching the perimeter to place IEDs. This would likely be result in a higher damager and destroyed rate, since IEDs do not cause widespread damage to transformers in this model.

4.8 Conclusions

The case study demonstrates an approach to evaluating infrastructure vulnerabilities and the efficacy of physical protection methods. The scenarios include

plausible attack scenarios based on real attacks, and address vulnerabilities to more sophisticated and coordinated attacks (particularly cyber-enabled attacks). While mitigation strategies proposed by private utilities and encouraged by NERC have the potential to greatly improve security standards across the nation's most critical and vulnerable electricity infrastructure sites, the results of this analysis demonstrate the importance of implementing effective security improvements. Concrete perimeter barriers around the sites and armored shielding around technical components such as transformers appear to be the most useful measures to prevent damage from a firearm attack.

The simulation is by no means complete: even for electrical substations, there may be other attack scenarios and system vulnerabilities not captured here. Future analysis could consider the feasibility and damage estimates from a multi-drone attack. This type of simulation has potential to be extended to different infrastructure components of the electric grid and other critical infrastructure sectors. Additionally, different kinds of attacks, methods, and assailant capabilities can be expanded into simulations. This analysis provides one basis, a starting point, for selecting among choices for physical protection upgrades, and for providing interim estimates of efficacy. Further work could link this type of model to cost benefit analysis or other decision frameworks for policymakers and industry officials. While utility sector experts may have advanced modeling and testing capability, the more general scenario developed through JCATS at Lawrence Livermore National Laboratory in this case study provides a basis for policymakers and other decision-makers to evaluate infrastructure vulnerability and attack countermeasures.

Acknowledgements:
Thank you to Nicholas Matyas with the Joint Conflict and Tactical Simulation (JCATS) team at Lawrence Livermore National Laboratory for hosting me, assisting in constructing the model, displaying the simulations. Additional thanks to Mark Piscotty, Hal Brand, Richard Grochowski, Brian Stevenson, and Joe Wilson for their insights and expertise that was integrated into the scenarios. Lastly, thank you to Jovana Helms and Nathaniel Gleason, of the Global Security E-Program at Lawrence Livermore National Laboratory, for making the arrangements for this research to be conducted at the lab.

CHAPTER 5. PUBLIC AND PRIVATE RESPONSE TO INCIDENTS IMPACTING CRITICAL INFRASTRUCTURE

5.1 Introduction

As defined by the Department of Homeland Security, there are sixteen sectors of critical infrastructure in the United States. When disasters occur and impact one or more of these sectors, what tends to be the policy response to these incidents? Are there commonalities, in terms of the scale of the subsequent response, across types of infrastructure? Here, we investigate the federal and state response to significant incidents across the United States' critical infrastructure sectors. This chapter aims to determine if there a link between the magnitude of significant events, such as natural disasters, accidents, illnesses, malicious events, or system failures, and the monetary federal or state response. Additionally, we ask if the response varies with the monetary cost of the event, or does it vary with the magnitude of the human health impact. The goal of this analysis is to examine how response funding is allocated across the critical infrastructure sectors and to investigate if some incidents receive larger amounts of funding support than others. That is to say, do all infrastructure sectors receive similar amounts of response funding if the impact across events are similar? Is there any discernable pattern? Particular attention is paid to significant incidents impacting the energy sector as it is arguably vital to the functionality and operation of all other critical infrastructure sectors. Therefore, this analysis also serves to evaluate whether the response to the energy sector consistent to the overall response across the other critical sectors.

Much of the research in the field of critical infrastructure disaster response centers around resiliency. However, "resiliency" in regard to risk mitigation, disaster response, and emergency management tends to have different meanings and definitions depending on the goal of the research (Bostick et al., 2017). Resiliency studies include researchers in the U.S. and internationally having studied conditions and determinants that help identify at what point during or after a disaster critical infrastructure will begin to break down (Boin and McConnell, 2007). Other research seeks to answer whether there is an effective baseline of disaster preparedness that would help mitigate damages from disasters (Cutter et al., 2010) or if modeling methods can help identify the most cost-effective mitigation strategies to be used in critical infrastructure protection plans (Scaparra and Church, 2006) (Bostick et al. 2016).

Prior research has shown a history of effective government disaster response but also acknowledges that severe breakdowns in the disaster response are possible, as evidenced with Hurricane Katrina in 2005 (Morris et al., 2007; Schneider, 2005) and, more recently, the ongoing crisis in Puerto Rico after 2017's Hurricane Maria. The type of disaster will impact crisis response, and the response will vary depending on the ability for the managing government to respond (Christensen et al., 2016). For example, research aimed at disaster resiliency in the Southeastern United States found that the region of a disaster impacts the communities resiliency to recovery, with urban areas far more resilient to disaster than their rural counterparts (Cutter et al., 2010). To improve disaster response across regions, regardless of socioeconomic factors or proximity to urban centers, research has emphasized improvements to the centralized federal emergency

management system (Lester and Krejci, 2007) and clear communication and direction that trickles down to the local level (Col, 2007).

In this article, instead of focusing on infrastructure resiliency, we are interested in learning more about response to major incidents that impact critical infrastructure. This chapter expands on this realm of study and considers response to disasters more broadly, including both government response, and the subsequent insured losses due to the events. Further novelty in this analysis is that we compare the magnitude of a disaster's impact monetarily in terms of both cost and human health impacts. As outlined in Dillon et al., 2014 article, including a range of magnitudes of events allows for a sense of federal response to events that could have been worse (a "near-miss").

We use a power-law scaling analysis to compare impact versus response for major incidents across the sixteen U.S. critical infrastructure sectors. Impact is measured first in the monetize cost to human health, and then measured in the initial monetary costs of the event. The response to a given disaster is measured in terms of funding, from both the Federal Emergency Management Agency (FEMA) allocations if applicable, as well as other funding allocated in response to the incident at the federal or state level. Additionally, we also compare the impact (monetary and human health) with the insured losses for the events, in order to examine how the costs of the significant events compare to what the insurance industry pays for.

This chapter first briefly introduces disaster response and previous research methods involving power-law scaling relationships. Next, a few aspects of the major incidents in the database are discussed, plus an explanation of the methods used for monetary estimates of responses, human health impacts, and cost impacts. The next

section presents the results of the analysis as well as a sensitivity analysis. The chapter concludes with a discussion and future implications for this research.

5.2 Background

5.2.1 Disaster Response

When a disaster, accident, or intentional malicious act impacts any of the sixteen critical infrastructure sectors, federal and state governments respond in a variety of ways. Federal response can be provided through FEMA as physical materials as well as monetary funding. Throughout its history, FEMA (originally established in 1984) has evolved to be a guiding force for disaster response management, research, and best practices for public administration (Comfort et al., 2012). FEMA provides funding in response to emergency declarations and major disaster declarations, both of which must first be declared an emergency or disaster by the Governor (or Tribal Chief Executive) and then the President. Emergency declarations are meant to provide emergency services and up to $5 million in supplemental assistance to the state or tribal government. Disasters are declared when damages are beyond the scope of the state or tribal government to handle on their own, and FEMA provides both emergency services and funding relief in the immediate aftermath as well as potentially long term assistance (such as rebuilding) (FEMA, 2018a).

There is sometimes a long delay in FEMA funding allocation reporting for both emergencies and major disaster declarations. For example, despite beginning declared an emergency in January of 2016, FEMA disaster assistance (in the form of clean water and water filtration materials) to Flint, Michigan's ongoing lead-contaminated water crisis has not ended and therefore total allocations are not yet known (FEMA, 2017a).

Conversely, not all incidents declared a FEMA disaster or emergency ultimately receive funding allocations (and instead only emergency services and materials), as evident with the Oklahoma City Bombing of 1995. Although declared a major disaster within a matter of days, FEMA but does not report any monetary assistance provided to the state (FEMA, 2004).

FEMA can also dictate and direct how funding assistance is spent after it is allocated. After the Oakland Hills Wildfire in 1991 (which had previously been the costliest wildfire in U.S. history until the Northern California fires in late 2017), FEMA provided approximately $5 million to the University of California at Berkeley and the City of Oakland to assist in fire mitigation strategies, namely the reduction of non-native and highly flammable vegetation (such as eucalyptus and pine trees). However, environmental groups such as the Sierra Club sued FEMA in 2015 on the grounds that non-native vegetation should not be reduced but instead entirely eliminated. In response, FEMA revoked the University and Oakland's access to the funds, instead allowing the State of California to use the funding assistance for fire-mitigation strategies as they see fit (Goldstein, 2018).

Aside from FEMA's monetary response to major incidents, another form of response may come from federal or state funding programs and agencies, or through policy response. While FEMA appears have only provided materials and emergency services after the Oklahoma City Bombing, the federal government provided the city with Community Development Block Grants and Small Business Grants (Kennedy, 2012). Similarly, Congress responded to the financial crisis in 2008 with the passing of the Emergency Economic Stabilization Act, which providing funding to bail out failing

banks (110th Congress, 2008). Another congressional response to the financial crisis was the American Recovery and Reinvestment Act, largely aimed at revitalizing many aspects of the critical infrastructure sectors (111th Congress, 2009). An example of state funding response can be seen in Michigan's handling of the ongoing water crisis. Since the crisis began in 2014 residents have been unable to safely drink tap water in their homes without use of filtration devices. To offset the costs of undrinkable water bills, the state has given more than $41 million to residents in the form of water utility credits (Dennis, 2017).

Major incidents that lead to a policy response rather than a funding allocation response include the *E. coli* outbreak of 1993 and the Tylenol tampering incident in 1982. In 1982, seven people were killed after Tylenol pill bottles were poisoned with arsenic (Mitchell, 1989). In 1983, Congress passed "the Tylenol Bill," in which citizens could now be tried with a federal offense if they were caught tampering with consumer products. Additionally, the Food and Drug Administration (FDA) in 1989 issued strict federal regulations for manufacturers to abide by in order to secure products could not be tampered with easily or without the consumer noticing (Markel, 2014). Similar policy response followed after four people died and 500 were sickened by *E. coli* contaminated hamburger meat in 1993 (Centers for Disease Control and Prevention, 1993). After renewed media attention to the incident in recent years, the Food Safety Modernization Act was signed into law in 2011, in which the FDA emphasizes prevention rather than response to food contamination crises (111th Congress, 2011).

5.3 Utilizing Power-Law Scaling Relationships to Evaluate Incident Impact

As this analysis considers a wide range of events, from Hurricane Katrina to the September 11th attacks, we consider power scaling as a way to compare the order of

magnitude differences that may occur between impact and response. Power-law scaling is widely used in studies across the natural sciences as a way to measure the relationship between a change in one variable and the subsequent change in the relating variable. For example, how changes to physical or social environments impact the communication patterns in Zebra finches (Ma et al., 2017), or how the amounts of sulphur, copper, and chlorine within a material leads to more or less dioxin emissions (Thomas and McCreight, 2008). Power-law scaling is not limited to the natural sciences, however, and has been used to study a variety of social science relationships. In the early and fast-growing days of the internet, power-law scaling helped explain how networks online expanded and how new branches of a network could be linked back to a single, well connected origin point (Barabasi and Albert, 1999).

More similar to this study, however, is J. Sylvan Katz's research involving the power-law relationships between organization size and impact of research. In his 2000 study, Katz employs power-scale laws to determine how the size of a research organization influences the impact, in terms of recognition and citations of papers published from the organizations (Katz, 2000).

*Table 5-1. Significant Events Across Critical Infrastructure Sectors *N/A indicates information is not available for incidents where if were either no injuries or injuries were not reported.*

Sector	Sector-Specific Agency	Significant Incident	Year	Impact (fatal)	Impacted (injury)*	Citation
Chemical	Department of Homeland Security	West Virginia Chemical Spill	2014	0	N/A	(Ward Jr., 2016)
Chemical	Department of Homeland Security	Tylenol Tampering	1982	7	N/A	(Mitchell, 1989)
Commercial Facilities	Department of Homeland Security	September 11th	2001	2996	N/A	(IAGS, 2004)
Communications & Information Technology	Department of Homeland Security	Y2K	2000	0	N/A	-
Critical Manufacturing	Department of Homeland Security	Hurricane Harvey	2017	68	N/A	(Walters, 2018)
Dams	Department of Homeland Security	Hurricane Katrina	2005	1833	N/A	(CNN Library, 2017)
Dams	Department of Homeland Security	Flooding in California (Levee Break)	2004	0	N/A	-
Defense Industrial Base	Department of Defense	Helicopter Crash in Iraq	2017	7	N/A	(Starr and Browne, 2018)
Emergency Services	Department of Homeland Security	Oakland Hills Wildfire	1991	25	150	(Lenihan, 2017)
Energy	Department of Energy	Northeast Blackout	2003	90	N/A	(Anderson and Bell, 2012)
Energy	Department of Energy	Metcalf	2013	0	N/A	-
Financial Services	Department of Treasury	Financial Crisis	2008	0	N/A	-
Food and Agriculture	Department of Agriculture, Department of Health & Human Services	E. coli O157:H7	1993	4	500	(Centers for Disease Control and Prevention, 1993)
Government Facilities	Department of Homeland Security, General Services Administration	Oklahoma City Bombing	1995	168	444	(Maningas et al., 1997)
Healthcare and Public Health	Department of Health and Human Services	Ebola	2015	11301	28,602	(USAID/OFDA Bulletin, 2016)

Healthcare and Public Health	Department of Health and Human Services	Zika	2016	0	5,601	(CDC, 2018)
Nuclear Reactors, Materials, and Waste	Department of Homeland Security	Three Mile Island	1979	0	N/A	(Nuclear Regulatory Commission, 2018)
Transportation Systems	Department of Homeland Security, Department of Transportation	Minnesota Bridge Collapse	2007	13	145	(Schaper, 2017)
Transportation Systems	Department of Homeland Security, Department of Transportation	Hurricane Sandy	2012	285	153	(Rettner, 2013)
Water and Wastewater Systems	Environmental Protection Agency	Flint Water Crisis	2014	12	N/A	(Dennis, 2017)

5.4 Data and Methodology

To conduct this analysis, we gathered information about significant incidents (such as natural disasters, accidents, and malicious acts) that occurred across the United States' critical infrastructure sectors. As defined by the Department of Homeland Security, there are 16 major critical infrastructure sectors in the U.S., with each sector being overlooked by one or more federal agencies (DHS, 2017). Table 5-1 lists the sectors with their associated agencies, as well as details about the significant events considered for the analysis. The incidents represent a mix of events; some that received extensive media coverage, some that did not. Some sectors have two separate examples included in the database, in order to compare notoriety amongst the incidents. All the incidents have a short-term, immediate cost associated with the incident, such as initial cleanup, evacuations, and security response costs. The majority of the incidents impacted human health either directly through fatalities or though injuries.

5.4.1 Data Selection

The incidents in this dataset were chosen based on three requirements. First, that the event clearly impacted at least one of the sixteen critical infrastructure sectors. Second, that the event was large enough in terms of magnitude of impact or response, and thus information and monetary data was available about the incident. This stipulation meant that there was moderate to large media coverage about the event, further confirming the magnitude of the incident. Third, that for each incident, there is data available for at least one measure of impact (human health or initial costs) and at least one measure of response (FEMA or other federal or state responses) or information for insured losses. There are many major incidents in the United States that individually impact human health, cause initial costly damages and insured losses, or require a federal or state response in assistance, but finding incidents that meet the three requirements above and clearly impact a specific critical infrastructure is more difficult.

To choose the incidents in the database, we began by including incidents within the last twenty years that met our requirements. When major incidents were still needed for some sectors, such as the Government Facilities sector and Nuclear Reactors, Materials, and Waste sector, the time range was expanded, thus adding the 1995 Oklahoma City Bombing and 1979 Three Mile Island to the dataset. Other incidents that were included due to the relevance and similarities they have with recent events for which data is not yet available. For example, the 1991 Oakland Hills was previously the costliest wildfire in U.S. history until the December 2017 Northern California wildfires (Lenihan, 2017). Similarly, the *e. Coli* outbreak from 1993 can be a useful comparison to the recent deadly outbreak in Spring of 2018 (Hoffman, 2018). Lastly, a similarity across

the Dam sector was the spillway failure at the Oroville dam in California in 2017 and the flooding that devastated an agriculture region in southern California in 2004 due to a levee failure (Fritz, 2017). In total, there are twenty-one major incidents, from 1979 to 2017, representing the sixteen critical infrastructure sectors. The only incident included where neither response nor insured loss information was available is the 2017 helicopter crash in Iraq, representing the Defense Industrial Sector (Starr and Browne, 2018). The military does not disclose insurance information about aircrafts (Government Accountability Office, 2015), nor has the military address the recent apparent rise in aviation accidents (Mizokami, 2018).

While not all the incidents occur solely in the United States (the Ebola outbreak in 2015 and Zika outbreaks in 2016), the response to the incident is only measured in terms of U.S. involvement. The responses considered in the dataset are federal funding allocated through FEMA, federal funding allocated through other sources (such as a federal or state agency), and insured losses (as reported after the incident). Due to the variety of the incidents, not all events resulted in each type of monetary response. And in some cases, such as the 2017 military helicopter crash in Iraq, government response data is not disclosed. The benefit of having a variety of incidents across the critical infrastructure sectors and a range of monetary responses (even when some are lacking) to each incident is that it allows us to compare responses to significant events across infrastructure sectors. All monetary values presented in the analysis are in constant 2017 U.S. dollars.

5.4.2 Monetarization of Human Health Impact

The aim of this analysis is to compare the impact, in terms of scope and scale, of significant incidents to the subsequent monetary response. First, human health impact is compared to the federal funding response of an incident (both FEMA and other federal or state funding allocations) and the insured losses of an incident. Next, the immediate costs of the incident are compared to the federal funding response (again, FEMA and other federal and state funding allocations) and then to the insured losses. Although data for FEMA funding and insured losses are readily available (when it was allocated), data for the immediate cost of an incident and the additional federal or state funding responses are more difficult to come by. Therefore, many sources were used to gather cost and response data in order to make the best possible estimate and to include the event in our analysis. FEMA has an annual budget allocation, which was $6 billion in 2017 (Naylor, 2017), based on the average cost of disasters over the past decade as well as an evaluation of the latest fiscal year's emergency spending (FEMA, 2017b). Major incidents that are declared an emergency can receive up to $5 million in funding assistance from FEMA, while there is not a set limit to assistance from FEMA for major disaster declarations (FEMA, 2018a). In addition, FEMA has an annual operation and basic preparedness base budget, which was $615 million in 2017 (FEMA, 2017b), to help finance recovery responses after an emergency. Not all major incidents that impact the critical infrastructure sectors are declared emergencies or major disasters and therefore do not receive FEMA funding. This is why we then consider federal response funding more broadly, as well as any state funding that is allocated for recovery costs.

Another factor that must be addressed is that in order to have this comparison, the human health impact is converted from fatalities, injuries, or direct disruptions to a monetary value. For this conversion, we use a minimally-modified version of the Value of a Statistical Life (VSL). We use the Value of a Statistical Life as a metric to fatalities because it is the chosen valuation measure across many of the federal agencies that overlook the Critical Infrastructure Sectors, including the Department of Transportation (DOT), the Environmental Protection Agency (EPA), the Food and Drug Administration (FDA), Department of Agriculture (USDA), and Health and Human Services (HHS) (Machina and Viscusi, 2014). The VSL provides a quantitative, monetary measurement of the "benefit of preventing injury or fatality" and is "defined as the additional cost that individuals would be willing to bear for improvements in safety" (Office of the Secretary of Transportation, 2016). To determine a single VSL for our analysis, we consider the agency-specific Value of Statistical Life for the DOT, USDA, FDA, HHS, and EPA and take the average value, as show in in Table 5-2 (Merrill, 2017; Office of the Secretary of Transportation, 2016). As a result, the VSL used here to quantify the human health impact of a fatality is $9.7 million in 2017 dollars. Overall, fatalities account for about 40% of the human health impacts.

Table 5-2. Agency-Specific Values of Statistical Life, in constant 2017 millions of dollars, used to estimate Human Health Impact (Merrill, 2017)

Agency-Specific Value of Statistical Life	Value ($M)
Department of Transportation	$9.8
Department of Agriculture	$9.1
Food and Drug Administration, Health and Human Services	$9.7
Environmental Protection Agency	$10.2
Average	$9.7

Table 5-3. Severity of Injury Human Health Impact monetary estimate, where cost is based on project 2020 Income Levels (Office of Air and Radiation, 2011)

Health Endpoint: Hospital Admissions	WTP
All respiratory (ages 65+)	$23,711
All respiratory (ages 0-2)	$10,002
Chronic obstructive Pulmonary Disease (COPD) (ages 65+)	$17,308
Asthma admissions (ages <65+)	$10,040
Pneumonia admissions (ages 65+)	$23,004
COPD, less asthma (ages 20-64)	$15,903
All cardiovascular (ages 65+)	$27,319
All cardiovascular (ages 20-64)	$29,364
Ischemic Heart Disease (ages 65+)	$33,357
Dysrhythmia (ages 65+)	$19,643
Congestive Heart Failure (ages 65+)	$19,619
Emergency room visits for Asthma	$396
Average	$19,139

The exact cause, severity, and length of stay in the hospital for the injuries in this dataset are not available. The causes and types of injuries vary from illnesses (the *E. coli* outbreak) to trauma (the Minnesota bridge collapse) to unknown (injuries from Hurricane Sandy). We assume that the injuries reported for each event are the number of patients that required visits to the hospital after the incident, as is seen with the *E. coli* outbreak in 1993 (Centers for Disease Control and Prevention, 1993). To quantify the impact of non-fatal injuries, we follow the guidance of the EPA's 2011 report, "The Benefits and Costs of the Clean Air Act from 1990-2020" (Office of Air and Radiation, 2011). The EPA uses a willingness-to-pay (WTP) approach to estimate the monetary amount a person would need to be compensated if exposed to an adverse health effect. Though the EPA uses the WTP estimates to then quantify premature death avoidance, we are interested in immediate health impacts for our dataset. Therefore, following the example of WTP in the Clean Air Act, we use the EPA's average non-lethal health impact values, of $19,000 per person, as an average WTP estimate for non-fatal health impacts, as displayed in Table 5-3 (Office of Air and Radiation, 2011). The estimated WTP to avoid or be

compensated for non-fatal injuries is based on the EPA's projected income levels for the year 2020. The monetary values for all incidents included in the dataset, associated with human health impact, initial cost of impact, FEMA response, other federal or state responses, and insured losses are displayed in Table 5-4.

Table 5-4. Monetary Impact, Response, and Insured Losses associated with major incidents impacting the critical infrastructure sectors. All values are in constant 2017 millions dollars.

Significant Incident	**Human Health Impact ($M)**	**Cost of Impact ($M)**	**FEMA Response ($M)**	**Other Fed. & State Response ($M)**	**Insured Loss ($M)**	**Citation**
West Virginia Chemical Spill		$151	$3		$158	(FEMA, 2014a; Raby, 2017; Ward Jr., 2016)
Tylenol Tampering	$68	$401			$234	(Markel, 2014; Mitchell, 1989)
September 11th	$29,052	$21,464	$8,872	$14,761	$45,078	(FEMA, 2001a, 2001b; iii Staff, 2014)
Y2K		$143,453		$10,336		(Bennett and Dodd, 1999; Lehman, 2000; Manjoo, 2009)
Hurricane Harvey	$659	$125,000	$6		$30,000	(FEMA, 2017c; Naylor, 2017; Walters, 2018)
Hurricane Katrina	$17,775	$125,000	$23,225		$79,703	(CNN Library, 2017; FEMA, 2015, 2005; Insured Losses, 2010; Katrina, 2018)
Flooding in California - Levee Break		$213	$42			(Breitler, 2014; FEMA, 2014b)
Helicopter Crash in Iraq	$68	$2				(Coop, 2018; Starr and Browne, 2018)
Oakland Hills Wildfire	$245	$2,707	$5		$2,700	(Cooper, 2017; Goldstein, 2018; U.S. Fire Administration, 1991)
Northeast Blackout	$873	$6,897	$27	$6,000	$238	(Assistance and Links, 2011; FEMA, 2010, 2009, 2008; Minkel, 2008; U.S.-Canada Power System Outage Task Force, 2004b)
Metcalf		$15		$300		(Pacific Gas and Electric, 2014)
Financial Crisis		$21,400,000		$23,000,000	$292,994	(Childress, 2012; Schich, 2009)

E. coli O157:H7	$48	$43			$57	(Brooks, 1993; Marler Clark Law, 2008; News Desk, 2017)
Oklahoma City Bombing	$1,638			$124	$323	(FEMA, 2004; Jenkins, 2018; Kennedy, 2012; LA Times, 1995)
Ebola Outbreak	$110,134	$2,100		$2,397		(FEMA, 2018b; USAID/OFDA Bulletin, 2016)
Zika Outbreak	$107		$25			(CDC, 2018; Kamoie, 2016)
Three Mile Island		$1,701			$94	(Nuclear Regulatory Commission, 2018; The Associated Press, 1993)
Minnesota Bridge Collapse	$129	$49	$7	$44	$56	(CNN Wire Staff, 2010; FEMA, 2012a; Minnesota Department of Transportation (MnDOT), 2008)
Hurricane Sandy	$2,767	$65,000	$18,370	$21,330	$29,200	(FEMA, 2018c, 2016, 2012b, 2012c, 2012d, 2012e, 2012f; "Most expensive hurricanes to the insurance industry worldwide from 2011 to 2016," 2017; Rettner, 2013)
Flint Water Crisis	$116	$87		$51		(Boyette, 2017; Fortin, 2017; Office of the Press Secretary, 2016)

Table 5-5 displays the total impact (human health and costs), the total public sector response (FEMA and other federal or state responses), and total private and public sector response (with insured losses being considered the private sector). All values are in millions of constant 2017 dollars. There is substantial uncertainty in the accounting of deaths, injuries, and monetary damages, and uncertainty in the monetization of deaths and injuries. We heavily relied of government data and reports whenever possible in order to include the best estimates of impact and response. When not available or not

reported upon, we relied on reputable media reports, peer reviewed journals, and books. For some events where fatalities were reported, we could not find reliable data accounting for injuries. A further note of uncertainty lies in our monetarization methods for human health impacts; there are a variety of options for estimating injuries, one of which is the EPA's WTP methods, but it is possible an alternative measurement may be better.

*Table 5-5. The total Impact, Total Public Response, and Total Public and Private Responses (Total Public Response plus insured losses. All values in constant 2017 millions of dollars. **Insured Losses Represents the Private Sector's Response.*

Significant Incident	Total Impact (Health + Cost) ($M)	Total Public Response (FEMA + Other Fed. & State) ($M)	Total Public & Private Response** ($M)
West Virginia Chemical Spill	$151	$3	$161
Tylenol Tampering	$469		$234
September 11th	$50,517	$23,633	$68,711
Y2K	$143,453	$10,336	$10,336
Hurricane Harvey	$125,659	$6	$30,006
Hurricane Katrina	$142,775	$23,225	$102,928
Flooding in California Result of a Levee Break	$213	$42	$42
Helicopter Crash in Iraq	$70		
Oakland Hills Wildfire	$2,952	$5	$2,705
Northeast Blackout	$7,770	$6,027	$6,265
Metcalf	$15	$300	$300
Financial Crisis	$21,400,000	$23,000,000	$23,292,994
E. coli O157:H7	$91		$57
Oklahoma City Bombing	$1,638	$124	$446
Ebola Outbreak	$112,234	$2,397	$2,397
Zika Outbreak	$107	$25	$25
Three Mile Island	$1,701		$94
Minnesota Bridge Collapse	$178	$51	$107
Hurricane Sandy	$67,767	$39,700	$68,900
Flint Water Crisis	$203	$51	$51

The aim of the analysis is to provide a broad overview of the response to major incidents impacting critical infrastructure, not necessarily to examine whether FEMA, the federal government, or state agencies fund certain kinds of disasters. We therefore graph the impact, first in terms of human health and then in terms of immediate costs, against the total response to the incident, as seen in Figure 5-1 and Figure 5-2 respectively, and to be explained in more detail in the Results section. (An additional breakdown of impact and FEMA response and impact and other federal or state responses is included in the Appendix.) Next, we again graph human health impact and cost impact against insured losses, as seen in Figure 5-3 and Figure 5-4 and explained in detail in the Results section. Due to the wide range in monetary values across incidents, we use a logarithmic scale for both the x- and y-axis.

We fit the data to a power law function. This appears as a straight line on a log-log plot. Given the wide scale of the data, from the range of disasters across critical infrastructure sectors to the response given the impact (human health or otherwise) of an event, it is important to also characterize the fit. Transforming the data in Table 5-4 and

Table 5-5 logarithmically, we then use linear least squares curve fit methods to calculate the statistical variance for the line along with the R^2 value to estimate goodness of fit. The output of this sensitivity analysis is described along with the result section below.

5.5 Results and Analysis

In the first comparison of monetary human health impacts (HHI) compared to the total public response (FEMA and other federal or state funding responses), we examine

major incidents that damaged critical infrastructure and caused fatalities or injuries. As seen in Figure 5-1 and scaled proportionally, the equation for the fitted line is:

$$\text{Public Response} = 0.21\ \text{HHI}^{\,1.05\pm0.3} \qquad (1)$$

There is ± 0.3 standard error in the scaling factor, ± 1.4 in the coefficient, and the R^2 value is 0.52. Here, the scaling of total funding response to human health impact is 1.05. This indicates that for the average funding response, the scaling is roughly 1-to-1, meaning that FEMA and the federal or state government agencies are responding, in terms of funding, roughly proportionally to the monetary human health impacts of the event, across the entire range of event scales.

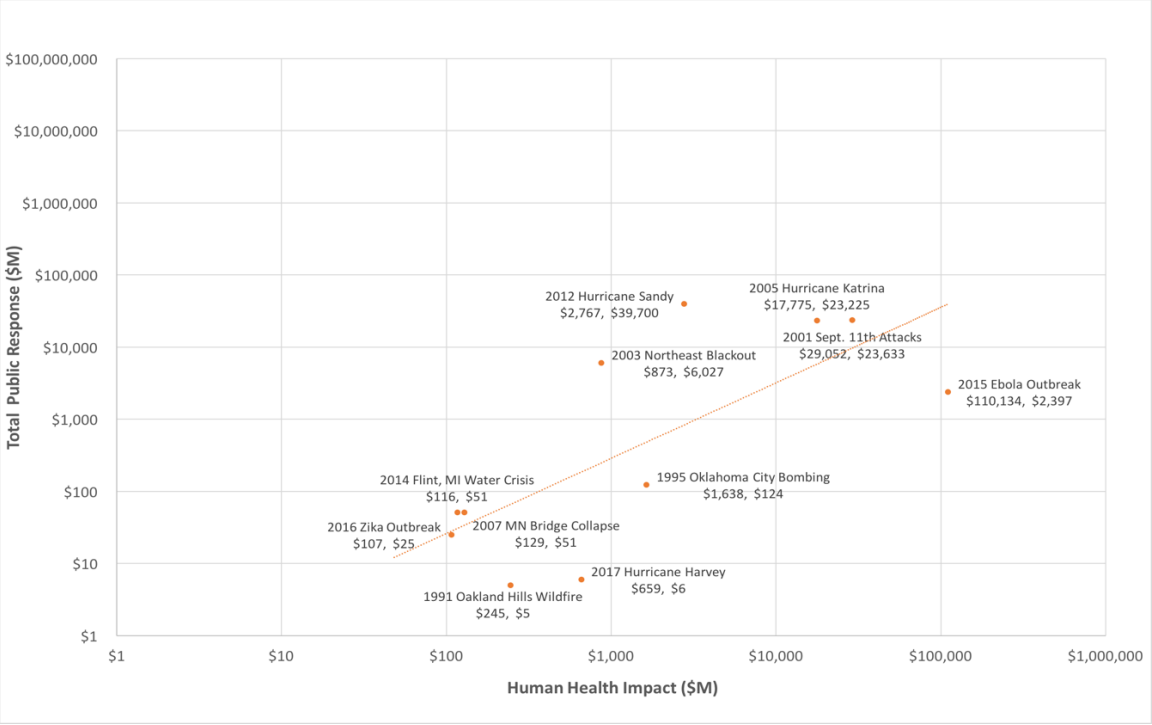

Figure 5-1. Human Health Impact ($M) and the Total Public Response (FEMA & Other) Allocated ($M) for major incidents impacting critical infrastructure.

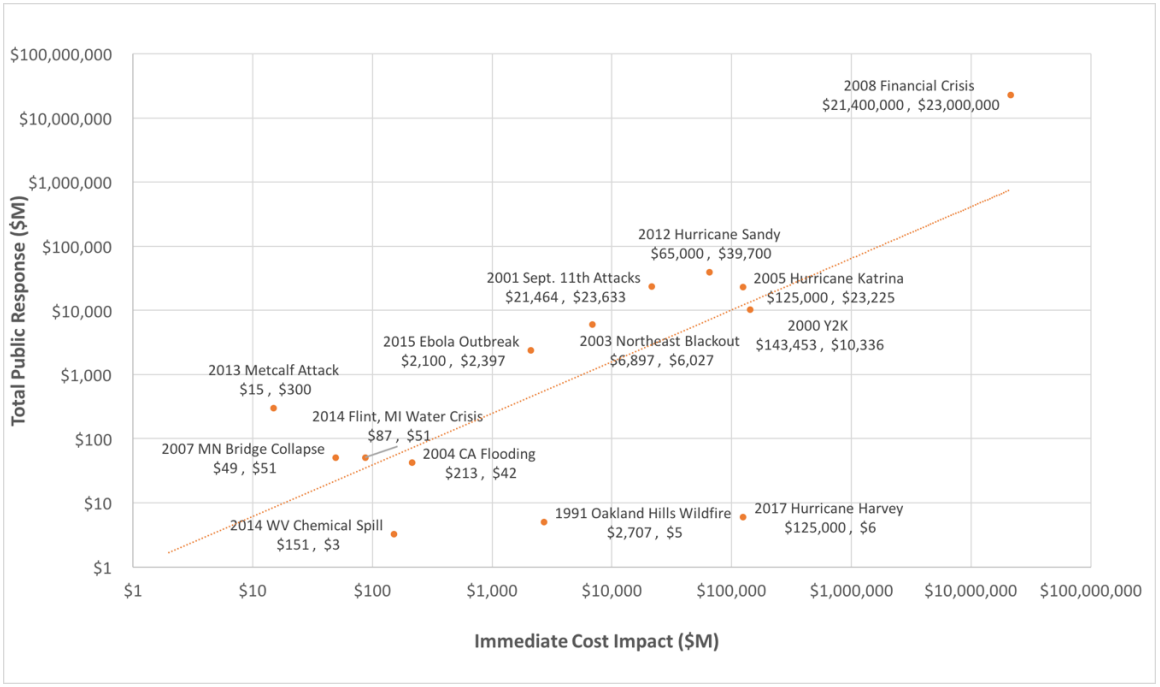

Figure 5-2. Immediate Cost Impact ($M) and the Total Public Response (FEMA & Other)

Allocated ($M) for major incidents impacting critical infrastructure.

Next, we examine the relatively immediate costs (IC) of the disaster (initial emergency response, short term funding) compared to the total public response (both FEMA and other federal or state agency responses) in Figure 5-2. Again scaling proportionally and finding the best fitted line, we have the following equation:

$$\text{Total Public Response} = 0.094\ IC^{\,0.81\pm0.23} \qquad (2)$$

Here, the initial costs of the event are not as linear to the total public response to a major event impacting critical infrastructure. The exponent for the power-law relationship is nearly 0.81, indicating that the response for events with a high initial impact cost receive relatively less than events with a low initial impact, with a scaling factor of 0.81 and standard error ± 0.23 scaling factor and ± 0.92 in the coefficient. The R^2 value is equal to 0.51.

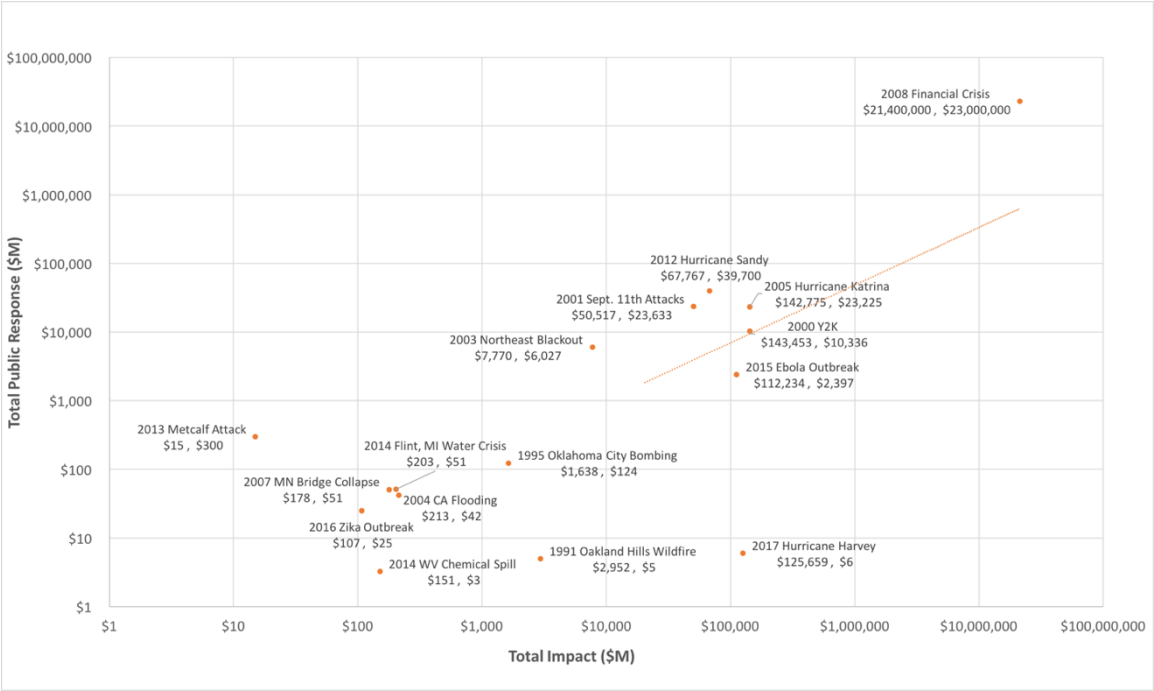

Figure 5-3. Total Impact (Human Health and Cost) ($M) and the Total Public Response (FEMA and Other Federal or State responses) ($M) for major incidents impacting critical infrastructure.

Figure 5-3 examines the relationship between the total impact, both human health and initial costs, of incidents and the subsequent total public sector response. The total public sector response to events with a high total impact receive slightly less than events with a low total impact, as scaled with the exponent value of 0.84 and a standard error of ± 0.2. The R^2 value is 0.56 and the coefficient has a standard error of ± 0.81.

$$\text{Total Public Response} = 0.44\ \text{Total Impact}^{0.84\pm0.2} \quad (3)$$

In the next set of figures, the insured losses associated with events are considered. In Figure 5-4, the human health impact of major incidents is compared with reported insured losses associated with the aftermath of the event. The resulting equation is:

$$\text{Insured Losses} = 1.64\ \text{HHI}^{1.05\pm0.3} \quad (4)$$

The exponent of 1.05 (with a standard error of ± 0.3) for the power-law relationship between human health impact and insured losses indicates that there is basically a linear response with insured losses being roughly 1.64 times the average human health impact that we have calculated. The R^2 value is 0.63 and the standard error on the coefficient is ± 0.87.

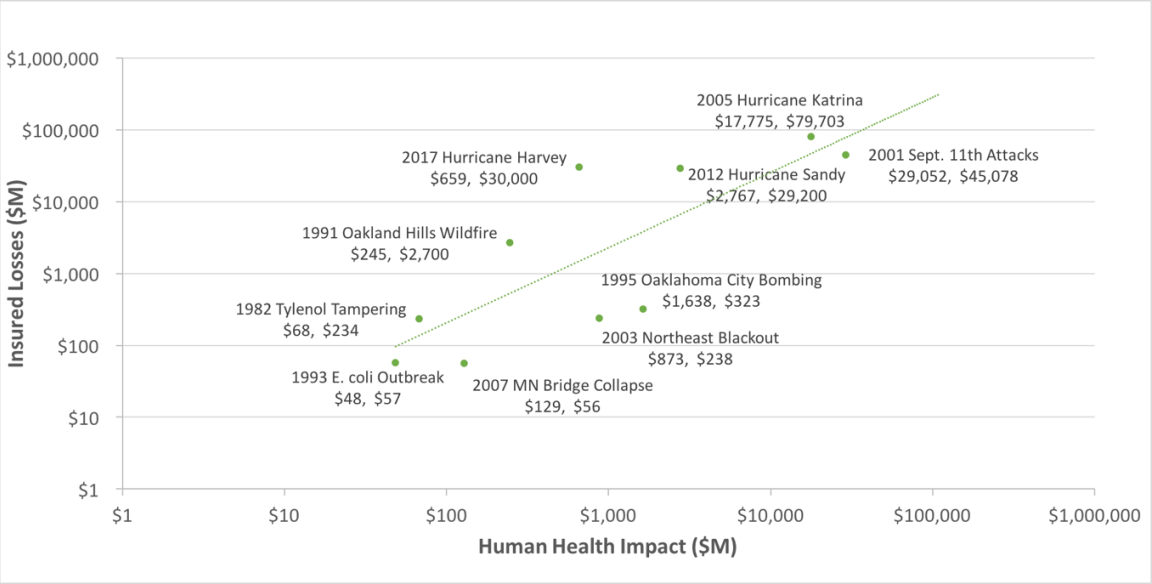

Figure 5-4. Human Health Impact ($M) and Insured Loss ($M) associated with major incidents impacting critical infrastructure.

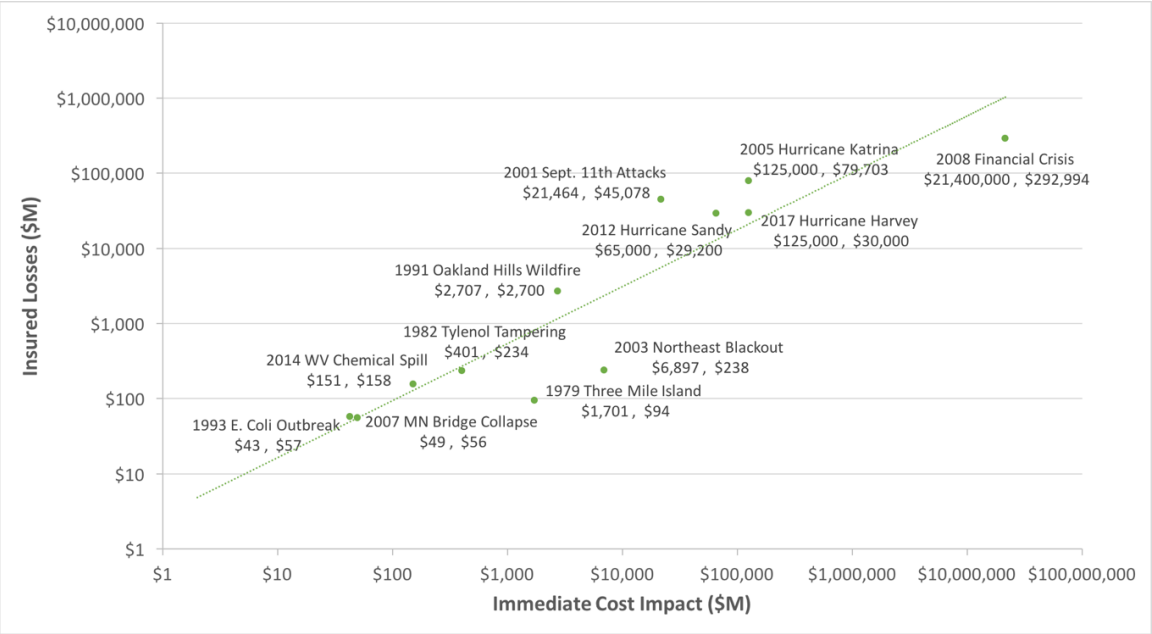

Figure 5-5. Immediate Costs ($) and Insured Loss ($M) associated with major incidents impacting critical infrastructure.

Conversely, the initial costs from the event compared to insured losses, seen in Figure 5-5, suggests that the immediate damages to infrastructure, buildings, or other material items after an event are not compensated as equally as human health impacts. Scaled proportionally and fitted with the best fit line, the equation is:

$$\text{Insured Losses} = 2.88\ IC^{\,0.76\pm0.11} \tag{5}$$

With an exponent of 0.76, it appears that events with high initial cost impacts after a disaster are reimbursed slightly less through insurance compared to low initial cost impacts, scaling at a factor of 0.76 and with a standard error of ± 0.15. The coefficient of 2.88 has a standard error of ± 0.44. The high R^2 here of 0.83 indicates that this model has a relatively high goodness of fit, especially compared to the previous models above.

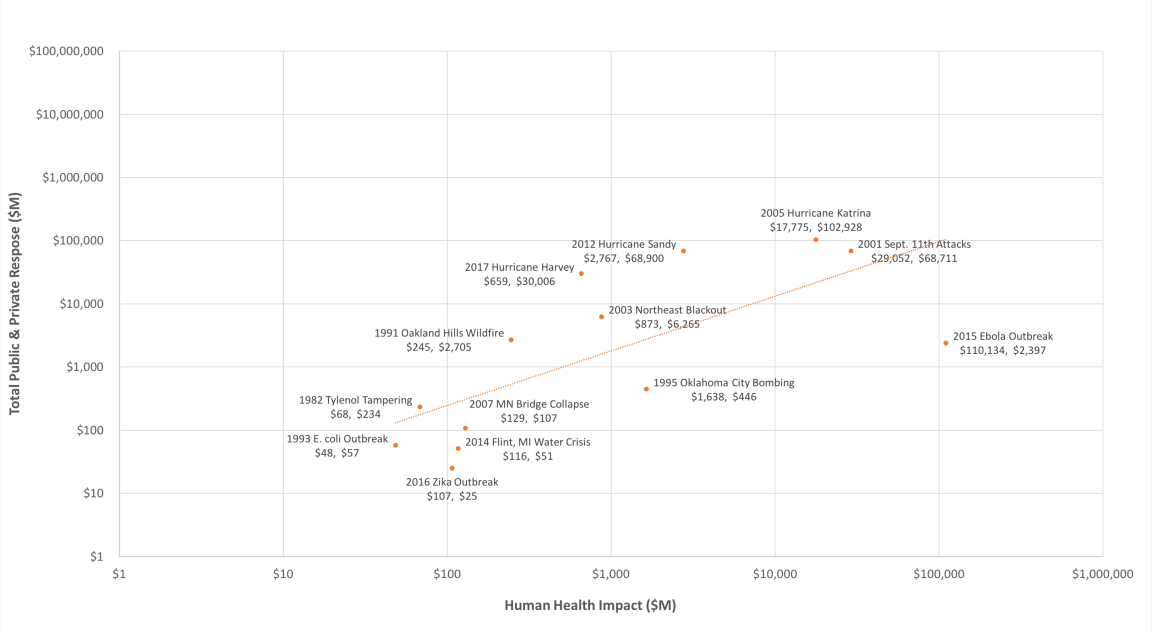

Figure 5-6. Human Health Impacts ($M) and Total Public and Private Response (FEMA and Other Federal or State funding responses, plus Insured Losses) Allocated ($M) for major incidents impacting critical infrastructure.

The final set of figures examine total response overall, meaning the combined public and private sector response. The public sector response is represented by FEMA and other federal or state funding, and the private sector response is represented by insured losses. Figure 5-6 depicts human health impacts compared to the public and private response. With a scaling factor of 0.87 (± 0.25), the results suggest that events with a higher human health impact receive slightly less funding than events with a high human health impact, with a scaling factor or 0.87. However, given a variance of ± 0.25, it is possible that the response is roughly linear to the impact. The coefficient has a standard error of ± 0.37 and an R^2 value of 0.52.

$$\text{Total Public \& Private Response} = 4.54\ HHI^{\,0.87\pm0.25} \qquad (6)$$

Results are similar for the total public and private sector response to major incidents compared to the resulting immediate cost impact. As shown in Figure 5-7, the response from the public and private sectors is slightly less for incidents with a high cost impact than for incidents where the cost impact is lower. The scaling factor is 0.89 and a standard error of ± 0.09 again suggests that the response may actually be closer to a 1-to-1 ratio with the cost impact. A high R^2 value of 0.87 suggests that much more of the variability in the data is explained in this particular model than the others. The coefficient of 1.82 has a standard error of ± 0.34.

$$\text{Total Public and Private Response} = 1.82\ IC^{\,0.89\pm0.09} \qquad (7)$$

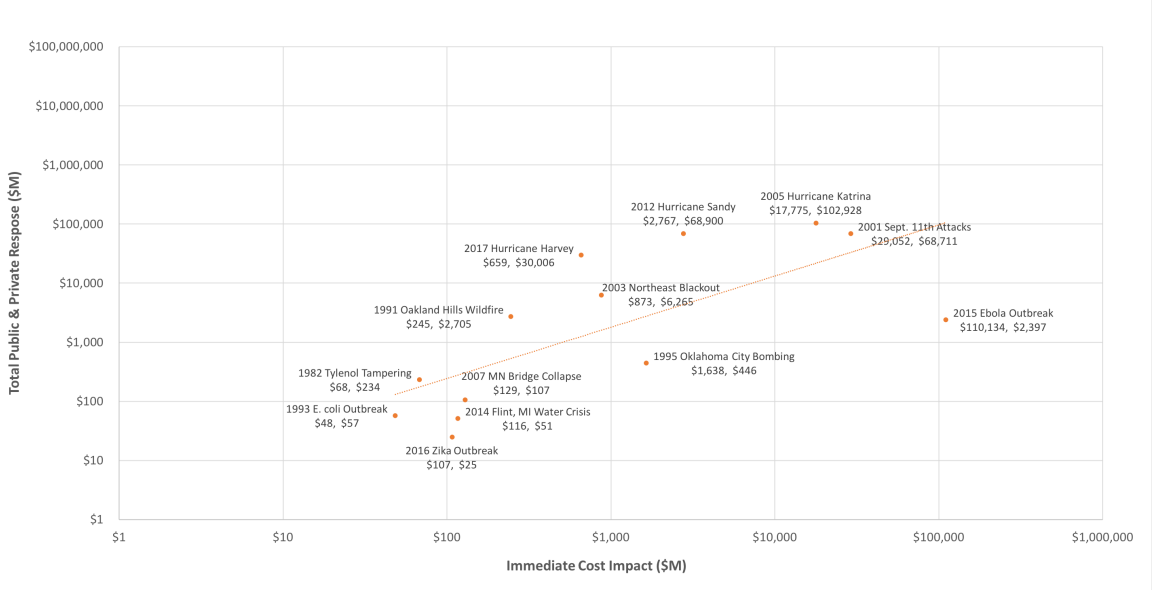

Figure 5-7. Immediate cost impacts and the Total Public and Private Response (FEMA and Other Federal or State funding responses, plus Insured Losses) Allocated ($M) for major incidents impacting critical infrastructure.

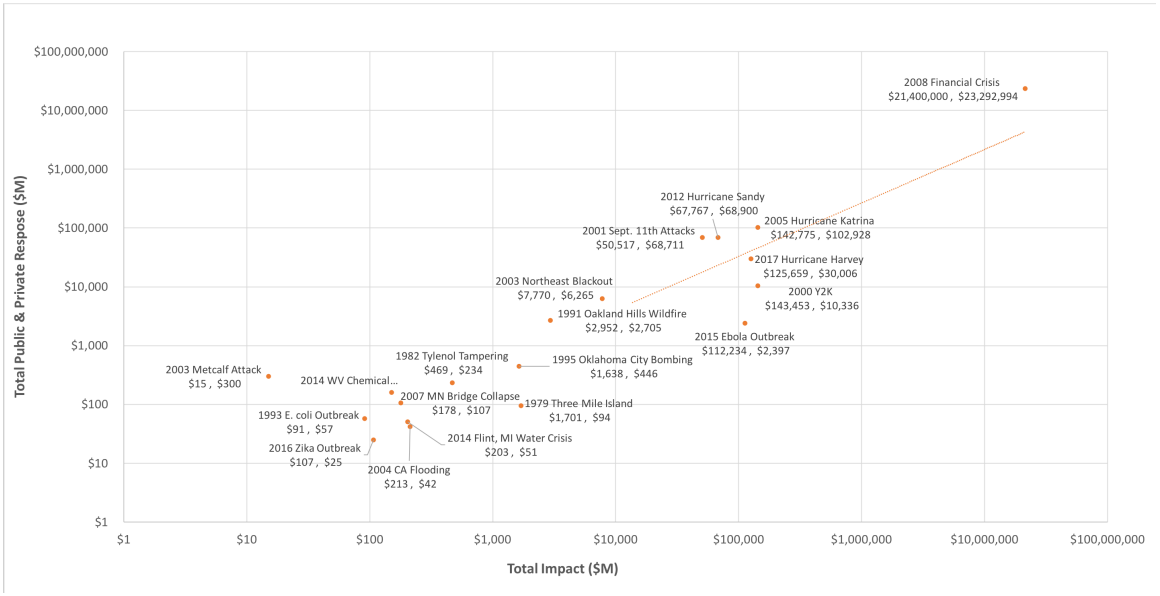

Figure 5-8. Total Impact (Human Health plus Cost) ($M) and the Total Public and Private Response (FEMA and Other Federal or State funding responses, plus Insured Losses) Allocated ($M) for major incidents impacting critical infrastructure.

Lastly, Figure 5-8 looks at the overall costs and the overall response, in terms of total impact (human health and cost) and total public and private sector response. A coefficient of 0.95 indicates a nearly 1-to-1 ratio between total impact and the subsequent response, with a standard error of ± 0.09. The high R^2 of 0.85 suggests that much of the variability in the data is explained in this model and the coefficient of 0.95 (with a standard error of ± 0.37), paired with a scaling factor of ± 0.9, indicates that the fit is nearly linear and with the overall response nearly equal to the calculated valuation of the financial and human health impacts.

$$\text{Total Public \& Private Response} = 0.95\ \text{Total Impact}^{\,0.9\pm0.09} \qquad (8)$$

5.6 Discussion

This analysis provides an overarching view across critical infrastructure sectors and examines the commonalities across the disaster response, in terms of scale or sector.

Broadly speaking, the public sector response to disasters is roughly proportional to the impact to human life, and to the immediate damages caused by the disaster. The relation of insured losses the human health impact (fatalities and injuries) and the immediate aftermath costs are also comparable.

There is interesting interaction between public sector response and private sector response. There are some incidents where the total public response was relatively low response but the private, insurance sector response was higher. This can be seen comparing Figure 5-1 and Figure 5-3 and observing the 1991 Oakland Hills Wildfire and Hurricane Harvey in 2017. Furthermore, some incidents did not receive a public sector response (other than policy change), such as the 1982 Tylenol Tampering incident and the 1993 *E. coli* Outbreak, while the insurance payments were substantial. This indicates that there are some events, or perhaps some sectors impacted, where insurance covers the majority of the response and the government does not, such as some natural disasters like wildfires and hurricanes. Additionally, there are possibly some sectors that are inherently privatized and face more of an insurance response when major incidents occur, such as the chemical sector and the food and agriculture sector. Due to the private sector nature of the sectors, the reasonable government response is through policy regulation, as evident from the "Tylenol Bill" and Food Safety Act to mitigate *e. coli* outbreaks.

The results for the model comparing total impact with total public and private response, as seen in Figure 5-8, helps show the relationship between the public and private sector response further. The model, with a high R^2 of 0.85, gives a fairly reasonable linear fit (scaling at 0.91±0.09), indicating a roughly 1-to-1 ratio of total impact to the subsequent total response. For some incidents, the public sector is the

designated responding sector, possibly due to the cause or the size of the disaster (e.g. the Ebola Outbreak in 2015) while other incidents that impact the private sectors or property receive more of an insurance response (Oakland Hills Wildfires). But for many disasters, it is a combination of public and private response, scaling at different levels depending on the incident or sector. Natural disasters tend to, but not always, receive high responses from both the public and private sectors, as do terrorist incidents like the Oklahoma City Bombing in 1995 and September 11th in 2001.

Additional observations are gained from the models that focus on a smaller scale, not necessarily total response or total impact. The results from the human health impact compared to total federal response analysis demonstrates that while disasters that kill or injure more people tend to receive the highest FEMA and other federal and state funding allocations in response, this is not always the case (Figure 5-1). For example, Hurricane Katrina resulted in far more fatalities than Hurricane Sandy and subsequently has a higher monetary human health impact. Yet the total federal response to Hurricane Sandy is slightly higher than that of Katrina. This raises two potential questions, the first being that perhaps region of the country influences funding response and second, perhaps income levels of the impacted regions influence funding response.

While all of the events included here received a moderate to high amount of media coverage during their respective time periods, the level of sensationalized reporting in the immediate aftermath of the events could possibly influence short term response allocations (Figure 5-2). For example, despite having similar costs, Hurricane Sandy received far more in total response allocations than Hurricane Harvey. In terms of how monetary responses compare across the different sectors, results suggest that the

sector impacted may have a slight influence over total response allocations from both FEMA and the federal and state agencies. Sectors associated with both high cost impacts and high social importance (the financial sector, transportation sector, information technology and communication sectors) are associated with large federal response allocations. These examples include the 2008 Financial Crisis, Hurricane Sandy, and Y2K). Hurricane Harvey in 2017, despite costing nearly as much in damages to the critical manufacturing sector in its immediate aftermath, received far less federal funding response.

For the Energy Sector, the 2003 Northeast Blackout and the 2013 Metcalf Substation Attack both impacted electricity delivery to major metropolitan areas (New York and Washington D.C., and Silicon Valley, respectively). However, the short term recovery costs to the Northeast Blackout were substantially higher given that length and geographical region of the outage and as such, the total response is also higher.

While a goal of this analysis was to pay particular attention to the energy sector, that aspect of the analysis proved difficult. Many major disasters that impacted the energy sector also impacted other critical infrastructure sectors, arguably more so than the energy sector. For example, while both Hurricane Katrina and Hurricane Sandy disrupted electricity reliability to the impacted regions, the damages to the dam sector (Katrina) and the transportation sector (Sandy) overshadow the possible costs associated with the energy sector. Moving forward with this research, it will be beneficial to include additional incidents that specifically impact mostly the energy sector. As it stands now, however, comparison between the Northeast Blackout and the Metcalf Attack is useful and does indicate that response to disasters that impact electricity reliability is consistent

with magnitude of the disaster as well as consistent with responses to other disasters across the infrastructure sectors.

5.7 Conclusion and Implications for Future Research

There are a wide range of major incidents included in this dataset and analysis; such will be the case when examining the sixteen different critical infrastructure sectors. Inherently when considering major disasters; each disaster is unique. This research looks at these incidents as a whole and seeks to determine patterns, similarities, and insights. This type of integrated, cross-infrastructure analysis can support the development of strategic guidance to public and private partners, for coordination of the overall Federal effort to promote the security and resilience of the nation's critical infrastructure (DHS, 2018).

The main patterns and insights to take away from this analysis are that the public sector tends to nearly respond proportionally given a disaster's impact to human health. Although the public sector responds less to high-cost impact disasters, it appears as though that's where the relationship with the private (insurance) sector comes into play. The government, through one avenue or another (FEMA or state agencies, for example), responds to some major incidents while the private, insurance sector responds to others. Furthermore, there are some disasters where the impact spans both initial costs and human health, and there is a combination of public sector and private sector response.

As this is a new approach to critical infrastructure response analysis, there are many potential avenues for future research. One option is to examine further whether socio-economic factors or political powers affect response. For example, do events in more wealthy regions or states receive a larger response to a disaster compared to poorer

areas? Or perhaps the political party in power nationally or regionally influence disaster response. A useful next step in this research field would be to develop the database, to include more events for each sector over all, large and small, with and without much media or political attention, to see how the response changes. This analysis and methods also can be applied to evaluate how other countries respond to disasters influence their critical infrastructure sectors.

CHAPTER 6. CONCLUSION

The resiliency, reliability, and security of electrical grid infrastructure is an ongoing issue and will continue to be threatened and tested by severe weather, failures, and malicious attacks. The overarching questions of focus for the dissertation research presented here are to determine what threats are impacting the electricity infrastructure in the U.S. and how policymakers respond. The research presented in this dissertation contributes to the overall understanding of threats to the grid, particularly concerning malicious attacks, including the evolution over time of such attacks. The retrospective analysis of attacks on the grid in Chapter 2 provides a robust assessment of the evolving methods and motivating factors of attack. How policymakers at the federal level respond to the threats of these attacks is measured in Chapter 3 using risk perception theory and time series regression analysis. The results of which offer a novel approach to using risk perception in a policy analysis setting. The vast amount of information gathered to create the incident databases used in this dissertation are put to further use in a modeling assessment in Chapter 4. Here, the model tests current and proposed grid security measures and mitigation strategies, ultimately offering meaningful data and information to utilities for where best to focus security efforts.

The final portion of the research, Chapter 5, questions whether the federal emergency response to disasters occurring in the energy sector, including electricity infrastructure, is in line with response across the other fifteen remaining critical infrastructure sectors. Contributing to the body of work regarding emergency response and management, this chapter takes new approach by categorizing disasters to specific

sectors and assessing the impact across both human health and financial impacts. The results show that response is proportional to the impact across each sector. The concluding remarks for this dissertation are presented below with an reiteration of each chapters research questions, methods, results, and impacts. Lastly, implications and possible directions for future research will conclude this body of work.

6.1 Targeted Attacks Against U.S. Electricity Infrastructure

There is a long history of attacks on electricity infrastructure in the United States, and it is important for future policy initiatives to understand both what the threats are and what reasons one may have to initiative an attack. As shown in Chapter 2, the motivations for and characteristics of the attacks provides insight into ongoing risks to the electric grid. I created a database of attacks against electricity infrastructure in the U.S. from 1970 to 2016, including the incident's date, location, method of attack, target type, severity of damage, success of the attack, and motivation. The seven motivation categories are: protest to a single focusing event; protest to U.S. foreign or military policy; protest for environmental reasons; acts of vandalism; acts of theft; acts to disrupt the government, economy, or utility; and acts of sabotage.

The data show a shift over the decades away from attackers communicating the motivation for their actions, to attacks that go unclaimed. This shift suggests that motivations change from protesting a specific event, policy, or government action to more general sabotage motivations. I included an additional classification for certain incidents that suggest an emergence of more sophisticated and coordinated attacks. Despite the current twenty-first century focus on cybersecurity, physical attacks remain

prevalent, therefore we recommend that states, utilities, and federal regulatory agencies recognize and mitigate physical vulnerabilities in addition to cybersecurity threats.

6.2 Federal R&D Funding Response to Incidents on the Grid

Based on the confirmed threats of targeted attacks against U.S. electricity infrastructure seen in Chapter 2, Chapter 3 investigated how policymakers are responding to malicious threats on the grid, particularly when compared to other regularly occurring threats such as weather events and human or technical failures. Using risk perception literature as a guide, I sought to determine whether the threat of targeted attacks to the Energy Sector, and therefore a perceived national security threat, lead to an increase in federal funding for grid-related research and development. I used the federally collected database of unusual disturbances on the grid, coded into risk categories, paired with the Energy and Water Appropriations Committee Reports as an indicator of risk perception. Next, the federal budget and allocations data for the Department of Energy's Office of Electricity was used as a measure of policy response to the given risks in a series of Finite Distributed Lag time series regression models.

The results of the analysis conclude that policymakers respond to disturbances caused by malicious events on the grid in approximately one year after the event. Furthermore, after controlling for large-impact events (in terms of media coverage or magnitude of the disturbance) the results show that policymakers respond with an increase in funding to malicious-related incidents regardless of media coverage, suggesting that policymakers are receiving other communications regarding the risks outside of media reports. The regression models do not indicate that policymakers are responding to weather-related or failure events on the grid, indicating that threats to

national security from attacks are considered a more pressing concern than naturally occurring weather events. Based on the Office of Electricity's funding trends, there is an increase in grid-related funding in recent years, and this could potentially be attributed to the growing number of cybersecurity incidents across critical infrastructure sectors, not just in the energy sector. Further evidence for this comes with the Department of Energy's newly created Office of Cybersecurity, Energy Security, and Emergency Response.

6.3 Will Updated Electricity Infrastructure Security Protect The Grid?

Considering that policymakers may have only recently begun putting more emphasis on grid security, I created a model in Chapter 4 to simulate attacks on a generic substation in order to understand the level of vulnerability electricity infrastructure currently faces given known feasible threats, as well as the infrastructure's vulnerability to potential future threats. Using data collected about past physical attacks from Chapter 2, feasible physical attacks are modeled against the updated security standards for a U.S.-based generic electric substation. A series of increasingly sophisticated physical attacks are simulated on the substation, as are a set of cyber-enabled physical attacks.

The findings indicate that some of the updated security measure are effective at mitigating damages to electrical infrastructure, while some are not. Specifically, additional barriers around the substation and physical armored protection of transformers reduce the amount of damage inflicted from both physical and cyber-physical attacks. In contract, additional cameras, sensors, and reduction in foliage are not as effective. This case study demonstrates an approach to testing the efficacy of physical security measures that can assist in decision-making for critical infrastructure security.

6.4 Public And Private Response To Incidents Impacting Critical Infrastructure

Chapter 5 considered critical infrastructure as a whole, investigating response to the impacts caused by major incidents across the sixteen Department of Homeland Security-defined critical infrastructure sectors. In this chapter, I created a database comprising of major natural disasters, accidents, malicious attacks, or other system failures, with each incident specific to the sector impacted the most due to the event. Impact of the events is measured monetarily in terms of human health (fatalities and injuries) and the initial costs associated with the impact. Response is measured in public sector response (FEMA and other federal or state agency responses) and private sector response (insured losses).

The results of this analysis indicate that the public sector response roughly proportionally to the human health impact of a disaster, as does the private sector. Furthermore, the results suggest that there may be some sectors, such as the Chemical and Food and Agriculture sector, where a privatization of the industries within it result a larger monetary private response than public response after disasters. Public response maybe instead be in the form of policy regulations, rather than monetary funding.

6.5 Future Outlook

The four research chapters presented here addressed the overarching question, what are the threats impacting the U.S. electric grid and how are policymakers responding, that grounds this dissertation, the potential for future research continues to grow. While threats range from severe weather to failures to malicious attacks, the research shows that malicious threats remain persistent and of concern to policymakers. Policymakers address

these concerns through policy priority initiatives in federal funding appropriations, and the results provide a new approach to policy analysis research that is in line with existing risk perception theory literature. The evolution and motivation behind malicious attacks is explored and modeled in detail against present and proposed security initiatives. Through a novel approach to federal emergency management and risk mitigation research, the analysis here indicates that federal emergency management is allocated in proportion to the impact of disasters across all critical infrastructure sectors.

Based on the methodologies, data usage, and results from the research presented here, there are many directions for future research. First, the methodologies of data collection practices can be applied to both a larger and smaller scale; in-depth analyses of threats at the local or state level, or an overarching informative study at the national level for other countries or regions, such as the European Union. In a continue use of risk perception theory, future studies can examine the roll a congress member's home state or geographical region plays in their perception to electric grid infrastructure threats. Specifically, do some policymakers from state's frequently impacted by natural disasters perceive severe-weather threats to be more pressing than risks related to failures or malicious attacks? Policy documents beyond Congressional Appropriations Committee Reports could be utilized here to provide insights into voting records and participation in other committees, beyond the Appropriations Committees. As security upgrades and risk mitigation strategies are implemented at high vulnerability and high priority electric grid infrastructure across the nation, further modeling efforts can be implemented to assess the monetary costs of these upgrades versus the potential monetary damages that could result from a malicious attack. Lastly, the field of federal emergency response research is

continuously growing and changing, and a particularly pertinent path of future research is to study risk mitigation and emergency response improvement in the face of climate change.

APPENDIX

Figure A-0-1 shows the separate breakdown of human health impacts ($M) compared to both FEMA funding response and other federal or state funding responses. The response allocated from FEMA appears to be roughly one and a half times the impact to human life, with a standard error of ± 0.4 calculated in the sensitivity analysis. The R^2 value is 0.75 and the coefficient 0.003 has a standard error of ± 1.15.

$$\text{FEMA Response} = 0.003\ \text{HHI}^{\,1.55\pm0.4} \tag{9}$$

The response allocated from other federal programs or state agencies is less than for incidents with high initial costs compared to events with lower initial costs. The scaling factor is 0.7 with a standard error of ± 0.4. Compared to the FEMA response, this indicates that the federal and state governments allocate less funding to compensate those who are adversely impacted, in terms of death or injury, from the disasters. However, the R^2 value is lower here, only 0.41. the standard error on the coefficient is ± 1.39.

$$\text{Other Federal \& State Response} = 5.22\ \text{HHI}^{\,0.7\pm0.4} \tag{10}$$

It is possible that the federal and state government funding is less than the FEMA response because the government preemptively plans for a potential FEMA response in their funding allocations (or this is already being captured).

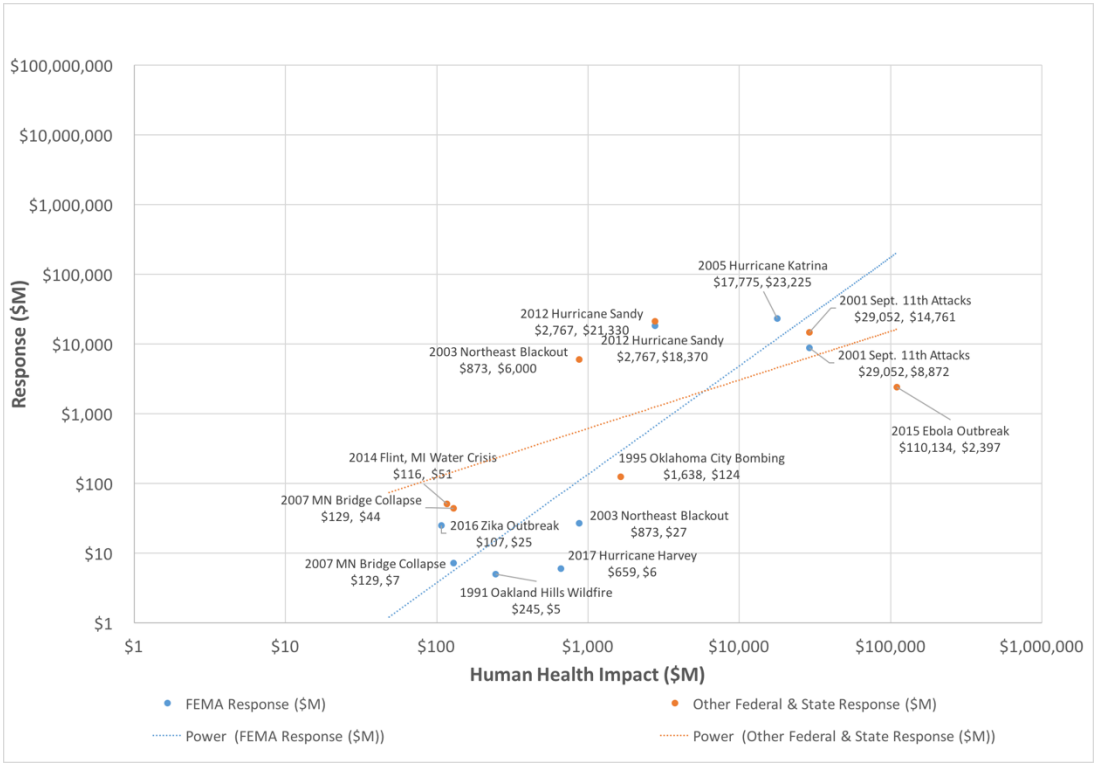

Figure A-0-1. Human Health Impact ($M) compared with both FEMA Response ($M) and Other Federal or State Responses ($M)

Figure A-0-2 displays the individual breakdown of immediate costs from the disaster ($M) again compared with both FEMA funding response and other federal or state funding responses. The response allocated from both FEMA and the federal or state government program and agencies is similar in this scenario, with FEMA responding slightly less to incidents that have a high initial cost compared to events with a lower initial cost after the impact. Here, the scaling factor is 0.76 with a standard error of ± 0.4. The R^2 value is 0.38 and the standard error on the coefficient is ± 1.43.

$$\text{FEMA Response} = 0.17\ IC^{\,0.78\pm0.4} \qquad (11)$$

Similarly, other federal government programs or state agencies respond slightly less to the costs large impact events compared to the of the cost of the lower impact events. Here, the scaling factor is 0.85 with a standard error of ± 0.1. the coefficient has a standard error of ± 0.55. The R^2 value here is 0.96.

$$\text{Other Federal \& State Response} = 3.29\ IC^{\,0.85\pm0.1} \qquad (12)$$

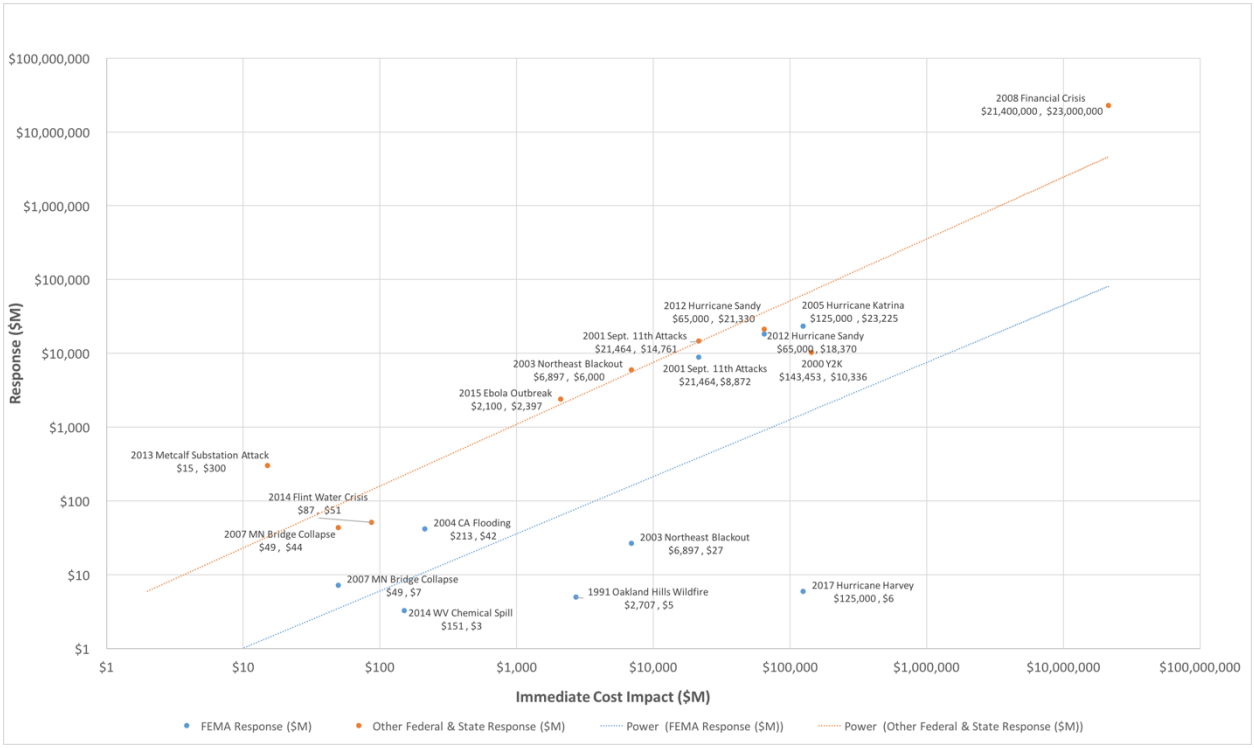

Figure A-0-2. Immediate Costs ($M) compared with both FEMA Response ($M) and Other Federal or State Responses ($M).

REFERENCES

109th Congress, 2005. Energy Policy Act of 2005. United States of America.

110th Congress, 2008. Emergency Economic Stabilization Act of 2008. 110th Congress, Washington D.C., United States of America.

111th Congress, 2011. FDA Food Safety Modernization Act. 111th Congress, United States of America.

111th Congress, 2009. American Recovery and Reinvestment Act of 2009. United States of America.

AAAS, 2018. Historical Trends in Federal R&D. Washington D.C.

Ackerman, G., Abhayaratne, P., Bale, J., Blair, C., Hansell, L., Jayne, A., Kosal, M., Lucas, S., Moran, K., Seroki, L., Vadlamudi, S., 2007. Assessing Terrorist Motivations for Attacking Critical Infrastructure. Monterey, CA.

Akerlof, K., Maibach, E.W., Fitzgerald, D., Cedeno, A.Y., Neuman, A., 2013. Do people "personally experience" global warming, and if so how, and does it matter? Glob. Environ. Chang. 23, 81–91. doi:10.1016/j.gloenvcha.2012.07.006

Alpas, H., Berkowicz, S.M., Ermakova, I., 2011. Environmental Security and Ecoterrorism. NATO Sci. Peace Secur. Ser. C Environ. Secur. 112, 15–29. doi:10.1007/978-94-007-1235-5

Anadon, L.D., Gallagher, K.S., Holdren, J.P., 2017. Rescue US energy innovation. Nat. Energy 2, 760–763. doi:10.1038/s41560-017-0012-0

Anderson, G.B., Bell, M.L., 2012. Lights out: Impact of the August 2003 power outage on mortality in New York, NY. Epidemiology 23, 189–193.

doi:10.1097/EDE.0b013e318245c61c

Apostolakis, G.E., Lemon, D.M., 2005. A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. Risk Anal. 25, 361–376. doi:10.1111/j.1539-6924.2005.00595.x

Assistance, F., Links, R., 2011. New York Power Outage (EM-3186) [WWW Document]. Fed. Emegency Manag. Agency - Emerg. Declar. URL https://www.fema.gov/disaster/3186

Associated Press, 2015. State regulators fine PG&E for failing to secure substation. Washingt. Times.

Associated Press, 2003. Suspect Held in Electric Tower Tampering. Los Angeles Times 1–2.

Atman, C.J., Bostrom, A., Fischhoff, B., Morgan, M.G., 1994. Designing Risk Communications: Completing and Correcting Mental Models of Hazardous Processes, Part I. Risk Anal. 14, 779–788.

Barabasi, A.-L., Albert, R., 1999. Emergency of Scaling in Random Networks. Science (80-.). 286, 509–513.

Baron, R.M., Kenny, D.A., 1986. The Moderator-Mediator Variable Distinction in Social Psychological Research. Conceptual, Strategic, and Statistical Considerations. J. Pers. Soc. Psychol. doi:10.1037/0022-3514.51.6.1173

Bennett, R.F., Dodd, C.J., 1999. Investigating the Impact of the Year 2000 Problem. The United States Senate, Washington D.C.

Boin, A., McConnell, A., 2007. Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. J. contingencies Cris.

Manag. 15, 50–59. doi:10.1111/j.1468-5973.2007.00504.x

Bostick, T.P., Holzer, T.H., Sarkani, S., 2017. Enabling Stakeholder Involvement in Coastal Disaster Resilience Planning. Risk Anal. 37, 1181–1200. doi:10.1111/risa.12737

Bostrom, A., Morgan, M.G., Fischhoff, B., Read, D., 1994. What Do People Know About Global Climate Change? 1. Mental Models. Risk Anal. 14, 959–970. doi:10.1111/j.1539-6924.1994.tb00065.x

Bowers, A., Prochnow, D.L., 2003. Multi-Resolution Modeling in the JTLS-JCATS Federation. Proc. IEEE fall Simul. Interoperability 1–11.

Boyette, C., 2017. Michigan and Flint agree to replace 18,000 home water lines by 2020. CNN 1.

Breitler, A., 2014. When the levee broke: In 10 years since devastating Jones Tract fooding, much has changed on Delta levees. RecordNet 1–2.

Brooks, N.R., 1993. Foodmaker Sees a Quarterly Loss : Fast food: Jack in the Box parent expects a $20-million to $30-million setback after poisonings, but says sales are rebounding. Los Angeles Times 1.

Brouillette, M., 2017. Heavy lifting drones fill a niche. Mech. Eng. 139, 23.

Brown, G., Carlyle, M., Salmerón, J., Wood, K., 2006. Defending critical infrastructure. Interfaces (Providence). 36, 530–544. doi:10.1287/inte.1060.0252

Burke, G., Fahey, J., 2014. AP Investigation: US power grid vulnerable to foreign hacks. Assoc. Press.

Burton-Rose, D., 2010. Creating a Movement with Teeth: A Documentary History of the George Jackson Brigade. PM Press.

California Public Utilities Commission, 2015. Enclosure 5 – PG & E Data Response 2, Supplement.

Campbell, R.J., 2012. Weather-Related Power Outages and Electric System Resiliency, CRS Report for Congress. Washington D.C.

Cantwell, M., 2015. Grid Modernization Act. 114th Congress, 1st Session.

Carter, C.J., 2013. Arkansas man charged in connection with power grid sabotage. CNN.

CDC, 2018. Cumulative Zika Virus Disease Case Counts in the United States, 2015-2018.

Centers for Disease Control and Prevention, 1993. Update: multistate outbreak of Escherichia coli O157: H7 infections from hamburgers--western United States, 1992-1993. MMWR. Morb. Mortal. Wkly. Rep. 42, 258.

Childress, S., 2012. How Much Did the Financial Crisis Cost? PBS 4–7.

Christensen, T., Lægreid, P., Rykkja, L.H., 2016. Organizing for Crisis Management: Building Governance Capacity and Legitimacy. Public Adm. Rev. 76, 887–897. doi:10.1111/puar.12558

Clarke, M.C., 2004. Terrorism, engineering and the environment: Their interrelationships. Terror. Polit. Violence 16, 294–304. doi:10.1080/09546550490483431

CNN Library, 2017. Hurricane Katrina Statistics Fast Facts. CNN 1–2.

CNN Wire Staff, 2010. Settlement reached in Minnesota bridge. Build. Up Am. 1–3.

Col, J.M., 2007. Managing disasters: The role of local government. Public Adm. Rev. 67, 114–124. doi:10.1111/j.1540-6210.2007.00820.x

Comfort, L.K., Waugh, Jr., W.L., Cigler, B.A., 2012. Emergency management research

and practice in public administration: Emerge...: EBSCOhost [WWW Document]. Public Adm. Rev. doi:10.1111/j.1540-6210.2012.02549.x

Conflict Simulation Laboratory, 2018a. Joint Conflict and Tactical Simulation (JCATS) Capabilities Brief. Livermore, CA.

Conflict Simulation Laboratory, 2018b. Conflict Simulation Laboratory, Joint Conflict and Tactical Simulation (JCATS). Livermore, CA.

Congress.gov, 2018. Energy and Water Appropriation Committee Reports [WWW Document]. Legis. Search Results - Committe Reports via Congr. URL https://www.congress.gov/search?searchResultViewType=expanded&q=%7B%22source%22%3A%22comreports%22%2C%22search%22%3A%22energy+and+water+appropriation%22%2C%22congress%22%3A%5B%22114%22%5D%2C%22chamber%22%3A%22Senate%22%7D

Coop, T., 2018. The death toll for rising aviation accidents: 133 troops killed in five years. Mil. Times 1–9.

Cooper, J.J., 2017. October's Wine Country Fires Were the Costliest Ever. Time Mag. 1–2.

Counterterrorism Threat Assessment and Warning Unit Counterterrorism Division, 1999. Terrorism in the United States - 1999.

Cutter, S.L., Burton, C.G., Emrich, C.T., 2010. Disaster Resilience Indicators for Benchmarking Baseline Conditions. J. Homel. Secur. Emerg. Manag. 7, 1–25. doi:10.2202/1547-7355.1732

Cyber Squirrel 1 [WWW Document], n.d. URL http://cybersquirrel1.com/

Dennis, B., 2017. Flint residents must start paying for water they still can't drink without

a filter. Washington Post 1.

Devost, M.G., Houghton, B.K., Pollard, N.A., 1997. Information terrorism: Political violence in the information age. Terror. Polit. Violence 9, 72–83. doi:10.1080/09546559708427387

Dews, F., 2014. Squirrels – A Bigger Threat than Cyber Terrorists? Brookings Inst. 1.

DHS, 2018. Critical Infrastructure Security [WWW Document]. Dep. Homel. Secur. URL https://www.dhs.gov/topic/critical-infrastructure-security

DHS, 2017. Critical Infrastructure Sectors [WWW Document]. Dep. Homel. Secur. URL http://www.dhs.gov/critical-infrastructure-sectors

Dillon, R.L., Tinsley, C.H., Burns, W.J., 2014. Near-misses and future disaster preparedness. Risk Anal. 34, 1907–1922. doi:10.1111/risa.12209

EIA, 2014. What is Energy: Forms of Energy – Basics [WWW Document]. URL http://www.eia.gov/energyexplained/print.cfm?page=about_forms_of_energy

Electricity Forum, 2015. Electrical Transformers Explained [WWW Document]. Electr. Forum. URL http://www.electricityforum.com/products/trans-s.htm

Ellis, P.D., 2014. Lone Wolf Terrorism and Weapons of Mass Destruction: An Examination of Capabilities and Countermeasures. Terror. Polit. Violence 26, 211–225. doi:10.1080/09546553.2014.849935

Energy.gov, 2018. Secretary of Energy Rick Perry Forms New Office of Cybersecurity, Energy Security, and Emergency Response [WWW Document]. Dep. Energy.

Energy.gov, 2017. About the Office of Electricity [WWW Document]. Off. Electr. Deliv. Energy Reliab. U.S. Dep. Energy, DOE/OE-0017. URL https://www.energy.gov/oe/about-office-electricity

FBI, 2018. Terrorism [WWW Document]. Fed. Bur. Investig. - What We Investig. URL https://www.fbi.gov/about-us/investigate/terrorism/terrorism-definition%0D

FBI, 2015. Attacks on Arkansas Power Grid Perpetrator Sentenced to 15 Years.

FEMA, 2018a. The Disaster Declaration Process [WWW Document]. Fed. Emegency Manag. Agency. URL http://www.fema.gov/declaration-process

FEMA, 2018b. Preparedness Grant Case Studies [WWW Document]. Fed. Emegency Manag. Agency. URL https://www.fema.gov/grant-case-studies

FEMA, 2018c. Delaware Hurricane Sandy (DR-4090) [WWW Document]. Fed. Emegency Manag. Agency - Major Disaster Declar. URL https://www.fema.gov/disaster/4090

FEMA, 2017a. Michigan Contaminated Water (EM-3375) [WWW Document]. Fed. Emegency Manag. Agency - Emerg. Declar. URL https://www.fema.gov/disaster/3375

FEMA, 2017b. Disaster Relief Fund: Monthly Report.

FEMA, 2017c. Louisiana Tropical Storm Harvey (DR-4345) [WWW Document]. Fed. Emegency Manag. Agency - Major Disaster Declar. URL https://www.fema.gov/disaster/4345

FEMA, 2016. New Hampshire Hurricane Sandy (EM-3360) [WWW Document]. Fed. Emegency Manag. Agency - Emerg. Declar. URL https://www.fema.gov/disaster/3360

FEMA, 2015. FEMA Outlines a Decade of Progress after Hurricane Katrina. Washington D.C.

FEMA, 2014a. West Virginia Chemical Spill (EM-3366) [WWW Document]. Fed.

Emegency Manag. Assoc. - Emerg. Declar. URL https://www.fema.gov/disaster/3366

FEMA, 2014b. California Flooding As A Result Of A Levee Break (DR-1529) [WWW Document]. Fed. Emegency Manag. Agency - Major Disaster Declar. URL https://www.fema.gov/disaster/1529

FEMA, 2012a. Minnesota Bridge Collapse (EM-3278) [WWW Document]. Fed. Emegency Manag. Agency - Emerg. Declar. URL https://www.fema.gov/disaster/3278

FEMA, 2012b. Connecticut Hurricane Sandy (DR-40 [WWW Document]. Fed. Emegency Manag. Agency - Major Disaster Declar. URL https://www.fema.gov/disaster/4087

FEMA, 2012c. District of Columbia (DC) Hurricane Sandy (DR-4096) [WWW Document]. Fed. Emegency Manag. Agency - Major Disaster Declar. URL https://www.fema.gov/disaster/4096

FEMA, 2012d. Maryland Hurricane Sandy (DR-4091) [WWW Document]. Fed. Emegency Manag. Agency - Major Disaster Declar. URL https://www.fema.gov/disaster/4091

FEMA, 2012e. New Jersey: Hurricane Sandy (DR-4086) [WWW Document]. Fed. Emegency Manag. Agency - Major Disaster Declar. URL https://www.fema.gov/disaster/4086

FEMA, 2012f. New York Hurricane Sandy (DR-4085) [WWW Document]. Fed. Emegency Manag. Agency - Major Disaster Declar. URL http://www.fema.gov/disaster/4085

FEMA, 2010. New Jersey Power Outage (EM-3188) [WWW Document]. Fed. Emegency Manag. Agency - Emerg. Declar. URL https://www.fema.gov/disaster/3188

FEMA, 2009. Ohio Power Outage (EM-3187) [WWW Document]. Fed. Emegency Manag. Agency - Emerg. Declar. URL https://www.fema.gov/disaster/3187

FEMA, 2008. Michigan Power Outage (EM-3189) [WWW Document]. Fed. Emegency Manag. Agency - Emerg. Declar. URL https://www.fema.gov/disaster/3189

FEMA, 2005. Mississippi Hurricane Katrina (DR-1604) [WWW Document]. Fed. Emegency Manag. Agency - Major Disaster Declar. URL https://www.fema.gov/disaster/1604

FEMA, 2004. Oklahoma Explosion at Federal Couthouse in Oklahoma City (DR-1048) [WWW Document]. Fed. Emegency Manag. Agency - Major Disaster Declar. URL https://www.fema.gov/disaster/1048

FEMA, 2001a. Virginia Terrorist Attack (DR-1392) [WWW Document]. Fed. Emegency Manag. Agency - Major Disaster Declar. URL https://www.fema.gov/disaster/1392

FEMA, 2001b. New York Terrorist Attack (DR-1391) [WWW Document]. Fed. Emegency Manag. Agency - Major Disaster Declar. URL https://www.fema.gov/disaster/1391

Fisher, E., Eto, J.H., LaCommare, K.H., 2011. Understanding bulk power reliability: The importance of good data and a critical review of existing sources. Proc. Annu. Hawaii Int. Conf. Syst. Sci. 2159–2168. doi:10.1109/HICSS.2012.611

Fortin, J., 2017. In Flint, Overdue Bills for Unsafe Water Could Lead to Foreclosures. New York Times 1–2.

Fritz, A., 2017. The Oroville Dam spillway failed miserably, so California is blowing it

up. Washington Post 1.

Giroux, J., Burgherr, P., Melkunaite, L., 2013. Research Note on the Energy Infrastructure Attack Database (EIAD). Perspect. Terror. 7, 113–125.

Gladstone, M., 2015. 2 Men Held in Alleged Plot to Bomb N. California Sites. Los Angeles Times 1–3.

Global Terrorism Database, 2015. National Consortium for the Study of Terrorism and Responses to Terrorism (START).

Goldstein, A.P., Narayanamurti, V., 2018. Simultaneous pursuit of discovery and invention in the US Department of Energy. Res. Policy 47, 1505–1512. doi:10.1016/j.respol.2018.05.005

Goldstein, D., 2018. Lessons learned — and ignored — from a fire that destroyed 3,450 homes. MarketWatch 1–8.

Government Accountability Office, 2015. Observations Related to Liability Insurance Requirements and Coverage for Aircraft Owners. Washington D.C.

Hamm, M.S., 2007. Terrorism As Crime From Oklahoma City to Al-Qaeda and Beyond. NYU Press, New York.

Hayes, C., 2014. Ferguson power outage caused by a vandal. Fox2Now.

Hewitt, C., 2005. Political Violence and Terrorism in Modern America: A Chronology. Praeger.

Hoffman, J., 2018. Four More People Die From Tainted Romaine Lettuce. New York Times 1.

Hoffman, P., Streit, D., 2015. United States Electricity Industry Primer. Off. Electr. Deliv. Energy Reliab. U.S. Dep. Energy, DOE/OE-0017 1–94. doi:DOE/OE-0017

Holding, R., 1999. Worker Gets 1-Year Sentence For Explosives Kept at PG&E [WWW Document]. SF Gate. URL http://www.sfgate.com/news/article/Worker-Gets-1-Year-Sentence-For-Explosives-Kept-2929742.php

Holstege, S., 2014a. "Suspicious device" explodes at Ariz. power plant [WWW Document]. USA Today. URL http://www.usatoday.com/story/news/nation/2014/06/11/suspicious-device-explodes-at-ariz-power-plant-/10354643/

Holstege, S., 2014b. "Suspicious device" explodes at Nogales power plant [WWW Document]. Repub. URL http://www.azcentral.com/story/news/arizona/2014/06/11/nogales-explosion-power-plant-arizona-abrk/10351107/

Holt, T.J., 2012. Exploring the intersections of technology, crime, and terror. Terror. Polit. Violence 24, 337–354. doi:10.1080/09546553.2011.648350

Homeland Security, 2014. Daily Open Source Infrastructure Report 17 June 2014.

IAGS, 2004. How much did the September 11 terrorist attack cost America? [WWW Document]. Inst. Anal. Glob. Secur. URL http://www.iags.org/costof911.html

iii Staff, 2014. Terrorism and Insurance: 13 Years After 9/11 The Threat of Terrorist Attack Remains Real. Insur. Inf. Inst. 11–14.

Ingraham, C., 2016. A terrifying and hilarious map of squirrel attacks on the U.S. power grid. Washington Post 1.

Insured Losses, 2010. Great Claims. Econ. 2–3.

James, B.D., 1981. Puerto Rican Terrorists Also Threaten Reagan Assassination. Lat. Am. Stud. 1–5.

Jarboe, J.F., 2002. Testimony: The Threat of Eco-Terrorism.

Jenkins, J.P., 2018. Oklahoma City Bombing. Britannica 1–5.

Judd, C.M., Kenny, D.A., 1981. Process analysis: Estimating Mediation in Treatment Evaluations. Eval. Rev. doi:10.1177/0193841X8100500502

Kamoie, B.E., 2016. Grant Programs Directorate Information Bulletin.

Kashubsky, M., 2011. Resources A Chronology of Attacks on and Unlawful Interferences with, Offshore Oil and Gas Installations, 1975 – 2010. Perspect. Terror. 5, 139–167.

Katrina, L.H., 2018. Louisiana Hurricane Katrina (DR-1603) [WWW Document]. Fed. Emegency Manag. Agency - Major Disaster Declar. URL https://www.fema.gov/disaster/1603

Katz, J.S., 2000. Institutional recognition. Science (80-.). 27, 23–36.

Kennedy, A., 2012. The Real Meaning of Community Service: The Economic and Financial Impact of the Oklahoma City Bombing. Edmond, OK.

Kincaid, J.P., Donovan, J., Pettitt, B., 2003. Simulation techniques for training emergency response. Int. J. Emerg. Manag. 1, 238. doi:10.1504/IJEM.2003.003300

Kittner, N., Lill, F., Kammen, D.M., 2017. Energy storage deployment and innovation for the clean energy transition. Nat. Energy 2, 1–6. doi:10.1038/nenergy.2017.125

Kocherlakota, N.R.., Yi, K.-M., 1996. A Simple Time Series Test of Endogenous vs . Exogenous Growth Models: An Application to the United States Source. Rev. Econ. Stat. 78, 126–134.

Kosal, M.E., 2006. Terrorism Targeting Industrial Chemical Facilities: Strategic Motivations and the Implications for U.S. Security. Stud. Confl. Terror. 29, 719–

751. doi:10.1080/10576100600702006

Kushner, H.W., 2002. Encyclopedia of Terrorism. Sage.

LA Times, 1995. OKLAHOMA CITY: AFTER THE BOMB : The Price Tag. Los Angeles Times 1.

Lawrence Livermore National Laboratory, 2017. Joint Conflict and Tactical Simulation (JCATS), Conflict Simulation Laboratory. Livermore.

Lebdetter, L., 1978. Page 7 Column 1. New York Times 1.

Lehman, D., 2000. Senate: Y2k Fixes Worth the Billions Spent. Computerworld 1–2.

Leiserowitz, A., 2006. Climate change risk perception and policy preferences: The role of affect, imagery, and values. Clim. Change 77, 45–72. doi:10.1007/s10584-006-9059-9

Leiserowitz, A., Smith, N., 2017. Affective Imagery, Risk Perceptions, and Climate Change Communication Summary and Keywords Affective Imagery, Risk Perceptions, and Climate Change Communication Affective Imagery, Risk Perceptions, and Climate Change Communication. Oxford Encycl. Clim. Sci. 1–29. doi:10.1093/acrefore/9780190228620.013.307

Lenihan, R., 2017. Northern California wildfires to be costliest in US history: Fitch. Bus. Insur. 1–3.

Lester, W., Krejci, D., 2007. Business “not” as usual: The national incident management system, federalism, and leadership. Public Adm. Rev. 67, 84–93. doi:10.1111/j.1540-6210.2007.00817.x

Lewinski, W.J., Avery, R., Dysterheft, J., Dicks, N.D., Bushey, J., 2015. The real risks during deadly police shootouts: Accuracy of the naive shooter. Int. J. Police Sci.

Manag. 17, 117–127.

Liu, W., Dugar, S., McCallum, I., Thapa, G., See, L., Khadka, P., Budhathoki, N., Brown, S., Mechler, R., Fritz, S., Shakya, P., 2018. Integrated Participatory and Collaborative Risk Mapping for Enhancing Disaster Resilience. ISPRS Int. J. Geo-Information 7, 68. doi:10.3390/ijgi7020068

Loadenthal, M., 2014. Eco-Terrorism? Countering Dominant Narratives of Securitisation: a Critical, Quantitative History of the Earth Liberation Front (1996-2009). Perspect. Terror. 8, 16–50.

Lopez, L., 1986. A PUZZLING CASE OF APPARENT NUCLEAR SABOTAGE. Assoc. Press 1–2.

Ma, S., Maat, A. Ter, Gahr, M., 2017. Power-law scaling of calling dynamics in zebra finches. Sci. Rep. 7, 1–11. doi:10.1038/s41598-017-08389-w

Machina, M.J., Viscusi, W.K., 2014. Risk and Uncertainty, in: Handbook of the Economics of Risk and Uncertainty. Elsevier, New York, pp. 602–643. doi:10.1007/978-1-4419-1191-9_12

MacNab, J., 2012. Sovereign Extremist Injured in Texas Bomb Explosion [WWW Document]. Forbes. URL http://www.forbes.com/sites/jjmacnab/2012/07/03/sovereign-extremist-injured-in-texas-bomb-explosion/

Macrotrends, 2017. Copper Prices - 45 Years Historical Chart [WWW Document]. Commod. Macrotrends, LLC. URL http://www.macrotrends.net/1476/copper-prices-historical-chart-data

Maningas, P.A., Robison, M., Mallonee, S., 1997. The EMS response to the Oklahoma

City bombing. Prehosp. Disaster Med. 12, 9–14. doi:10.1017/S1049023X0003733X

Manjoo, F., 2009. Apocalypse Then: Was Y2K A Waste? Slate Mag. 1–4.

Margolis, R.M.., Kammen, D.M.., 1999. Underinvestment: The Energy Technology and R&D Policy Challenge. Am. Assoc. Adv. Sci. 285, 690–692.

Markel, H., 2014. How the Tylenol murders of 1982 changed the way we consume medication. PBS News Hour 1–2.

Markey, E., 2010. Grid Reliability and Infrastructure Defense Act. 111th Congress, 2nd Session.

Marler Clark Law, 2008. Jack in the Box E. coli Outbreak Lawsuits - Western States (1993) [WWW Document]. Food Litig. URL http://www.marlerclark.com/case_news/view/jack-in-the-box-e-coli-outbreak-western-states

Massoud, A., 2003. North America's Electricity Infrastructure: Are we ready for more perfect storms?, in: IEE Security & Privacy. IEEE Computer Society, pp. 19–25.

Mathias, J.-D., Clark, S., Onat, N., Seager, T., 2018. An Integrated Dynamical Modeling Perspective for Infrastructure Resilience. Infrastructures 3, 11. doi:10.3390/infrastructures3020011

Merrill, D., 2017. No One Values Your Life More Than the Federal Government. Bloomberg 1–8.

Minkel, J., 2008. The 2003 Northeast Blackout--Five Years Later. Sci. Am. 3–6.

Minnesota Department of Transportation (MnDOT), 2008. Economic Impacts of the I-35W Bridge Collapse.

Mitchell, M.L., 1989. The Impact of External Parties on Brand-Name Capital: The 1982

Tylenol Poisonings and Subsequent Cases. Econ. Inq. 27, 1–18.

Mizokami, K., 2018. What's Behind the Stark Rise in U.S. Military Accidents? Pop. Mech. 1–5.

Montalbano, W.D., 1996. British Claim Raids Thwart IRA Bomb Plot. Los Angeles Times.

Morris, J.C., Morris, E.D., Jones, D.M., 2007. Reaching for the philosopher's stone: Contingent coordination and the military's response to Hurricane Katrina. Public Adm. Rev. 67, 94–106. doi:10.1111/j.1540-6210.2007.00818.x

Most expensive hurricanes to the insurance industry worldwide from 2011 to 2016 [WWW Document], 2017. . Statista. URL https://www.statista.com/statistics/281029/costliest-storms-for-the-insurance-industry-worldwide/

Murkowski, L., 2015. Energy Policy Modernization Act. 114th Congress, 1st Session.

National Research Council of the National Academies, 2012. Terrorism and the Electric Power Delivery System: Committee on Enhancing the Robustness and Resilience of Future Electrical Transmission and Distribution in the United States to Terrorist Attack. Washington D.C.

Naylor, B., 2017. With Harvey And Now Irma, Federal Funds And FEMA Are Put To The Test. NPR 1–10.

Nemet, G.F., Kammen, D.M., 2007. U.S. energy research and development: Declining investment, increasing need, and the feasibility of expansion. Energy Policy 35, 746–755. doi:10.1016/j.enpol.2005.12.012

NERC, 2014. Project 2014-04 Physical Security [WWW Document]. North Am. Electr.

Reliab. Corp. URL http://www.nerc.com/pa/Stand/Pages/Project-2014-04-Physical-Security.aspx

News Desk, 2017. Jack in the Box E. coli Outbreak – 25th Anniversary. Food Saf. News 1–3.

North American Electricity Reliability Corporation, 2016. State of Reliability 2016. Atlanta.

North American Electricity Reliability Corporation, 2015a. CIP-014-2 Physical Security.

North American Electricity Reliability Corporation, 2015b. Physical Security Standard Implementation [WWW Document]. NERC Phys. Secur. Stand. Implement.

North American Electricity Reliability Corporation, 2014. Statement on Physical Security. Atlanta.

Nuclear Regulatory Commission, 2018. Nuclear Insurance and Disaster Relief Nuclear Insurance: Price-Anderson Act [WWW Document]. Off. Public Aff. URL https://www.nrc.gov/docs/ML0327/ML032730606.pdf

Office of Air and Radiation, 2011. The Benefits and Costs of the Clean Air Act from 1990 to 2020 Final Report.

Office of Electricity Delivery & Energy Reliability, 2018a. Electric Disturbance Events (OE-417) [WWW Document]. Dep. Energy. URL http://www.oe.netl.doe.gov/oe417.aspx

Office of Electricity Delivery & Energy Reliability, 2018b. Congrssional Budget Resquest for OE [WWW Document]. Energy.gov. URL https://www.energy.gov/oe/about-us/budget

Office of Electricity Delivery & Energy Reliability, 2012. Large Power Transformers and

the U.S. Electric Grid. Washington D.C.

Office of the Press Secretary, 2016. FACT SHEET: Federal Support for the Flint Water Crisis Response and Recovery. White House Press Release 1–5.

Office of the Secretary of Transportation, 2016. Guidance on Treatment of the Economic Value of a Statistical Life (VSL) in U.S. Department of Transportation Analyses - 2016 Adjustment. Washington D.C.

Pacific Gas and Electric, 2014. PG&E Announces Reward For Information On Metcalf Substation Attack. PG&E News Releases 1.

Page 17 Column 1, 1977. . New York Times Page 17 Column 1.

Pala, C., 2015. Terrorists blow up power station. United Press Int. 1–7.

Parfomak, P.W., 2018. NERC Standards for Bulk Power Physical Security: Is the Grid More Secure? Washington D.C.

Paulo, E.P., Jimenez, R., Rowden, B., Causee, C., 2010. Simulation Analysis of a System to Defeat Maritime Improvised Explosive Devices (MIED) in a US Port. J. Def. Model. Simul. Appl. Methodol. Technol. 7, 115–125. doi:10.1177/1548512910365849

Perry, D., 2015. “Days of Rage” scorns George Jackson Brigade, but Northwest radical group won’t be ignored [WWW Document]. Oregon Live. URL http://www.oregonlive.com/living/index.ssf/2015/04/days_of_rage_scorns_george_jac.html

Post, J.M., Ruby, K.G., Shaw, E.D., 2000. From Car Bombs to Logic Bombs: The Growing Threat from Information Terrorism. Terror. Polit. Violence 12, 97–122. doi:10.1080/09546550008427563

Public Health and Welfare, 2001. Critical Infrastructure Protection Plan. Office of Inspector General-Health Care, Department of Health and Human Services.

Raby, J., 2017. Many Hands Await $151M West Virginia Chemical Spill Payout. Insur. J.

Register, C., 2015. Former FERC Chief Jon Wellinghoff Speaks Out on Grid Security and Distributed Generation. Forbes Mag. 1–7.

Rettner, R., 2013. Hurricane Sandy's Toll on Health. Live Sci. 1–5.

Rippl, S., 2011. Cultural theory and risk perception : a proposal for a better measurement Cultural theory and risk perception : a proposal. J. Risk Res. 37–41. doi:10.1080/1366987011004259

Rosen, A., 2016. Incendiary devices found hanging on Tyngsborough power lines. Boston Globe.

Salmeron, J., Wood, K., Baldick, R., 2004. Analysis of Electric Grid Security Under Terrorist Threat Under Terrorist Threat. IEEE Trans. Power Syst. 19, 905–912.

Sarbanes, J., 2015. 21st Century Power Grid Act. 114th Congress, 1st Session.

Scaparra, M.P., Church, R.L., 2006. A bilevel mixed-integer program for critical infrastructure protection planning. Comput. Oper. Res. 35, 1905–1923. doi:10.1016/j.cor.2006.09.019

Schaper, D., 2017. 10 Years After Bridge Collapse, America Is Still Crumbling. Natl. Public Radio 1–11.

Schich, S., 2009. Insurance Companies and the Financial Crisis. Financ. Mark. Trends 2009, 1–31. doi:10.1787/fmt-2009-5ks5d4npxm36

Schneider, S.K., 2005. Administrative breakdowns in the governmental response to

Hurricane Katrina. Public Adm. Rev. 515–516.

Security Sales and Integration, 2014. PG&E to Spend $100M to Upgrade Security After Substation Breach [WWW Document]. Secur. Sales Integr. URL http://www.securitysales.com/article/pge_to_spend_100m_to_upgrade_security_after_substation_breach

Serrano, R.A., Halper, E., 2014. Sophisticated but low-tech power grid attack baffles authorities. Los Angeles Times 1–5.

Shumard, R., 2015. Utilities Look to Get Started with NERC CIP-014-1 Physical Security Standard [WWW Document]. Energy Biz. URL http://www.energybiz.com/article/15/02/utilities-look-get-started-nerc-cip-014-1-physical-security-standard

Sissine, F., 2015. DOE's Office of Energy Efficiency and Renewable Energy: FY2016 Appropriations. Washington D.C.

Sjoberg, L., 2000. Factors in risk perception. Risk Anal. 20, 1–11. doi:10.1111/0272-4332.00001

Slovic, P., Peters, E., 2006. Risk perception and affect. Curr. Dir. Psychol. Sci. 15, 322–325. doi:10.1177/03063127067078012

Smith, R., 2014a. U.S. Risks National Blackout From Small-Scale Attack. Wall Str. J.

Smith, R., 2014b. Assault on California Power Station Raises Alarm on Potential for Terrorism. Wall Str. J. 1–7.

Sovacool, B.K., Brown, M.A., 2010. Competing Dimensions of Energy Security: An International Perspective, Annual Review of Environment and Resources. doi:10.1146/annurev-environ-042509-143035

Starr, B., Browne, R., 2018. 7 US service members killed in Iraq helicopter crash. CNN 1.

Sterlacchini, A., 2012. Energy R&D in private and state-owned utilities: An analysis of the major world electric companies. Energy Policy 41, 494–506. doi:10.1016/j.enpol.2011.11.010

Terrorist Unit Resurfaces, Claims Power Plant Blast, 1978. . Washington Post A3.

The Associated Press, 1993. 14-Year Cleanup at Three Mile Island Concludes. New York Times 1001019.

Thomas, J., 1981. PUERTO RICO TERRORIST GROUP TAKES RESPONSIBILITY FOR BLACKOUT. New York Times.

Thomas, V.M., McCreight, C.M., 2008. Relation of chlorine, copper and sulphur to dioxin emission factors. J. Hazard. Mater. 151, 164–170. doi:10.1016/j.jhazmat.2007.05.062

U.S.-Canada Power System Outage Task Force, 2004a. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations.

U.S.-Canada Power System Outage Task Force, 2004b. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, Security Working Group (SWG) Final Report. Washington D.C.

U.S. Fire Administration, 1991. The East Bay Hills Fire Oakland-Berkeley, California. Oakland-Berkeley, CA.

U.S. NRC, 2015. Frequently Asked Questions About Force-on-Force Security Exercises at Nuclear Power Plants [WWW Document]. Nucl. Regul. Comm. URL http://www.nrc.gov/security/faq-force-on-force.html

Us, A., 1971. Explosion Rocks Stanford Offices. The Harvard Crimson 1–2.

USAID/OFDA Bulletin, 2016. West Africa - Ebola Outbreak Fact Sheet #6, Fiscal Year (FY) 2016, Centers for Disease Control and Prevention (CDC).

Valencia, M.J., 2016. Man vowed ‘war’ in letter left with incendiary devices in Tyngsborough. Boston Globe.

Wald, M.L., 2014. California Power Substation Attacked in 2013 Is Struck Again. New York Times 1–3.

Walters, J., 2018. Harvey was second-most expensive US hurricane on record, official report says. Guard. 1–2.

Ward Jr., K., 2016. WV water crisis settlements provide community up to $151M. Charlest. Gazette-Mail 1–4.

Watson, J., 2012. 2011 Blackout In San Diego, Parts Of Arizona & Baja California Blamed On “Inadequate Planning.” Huffingt. Post 1–2.

Wheaton, L., 1980. Power back to normal in Puerto Rico. Lawrence J. 1.

Wigglesworth, V., 2015. Plano man gets maximum 20-year sentence for putting explosive on pipeline [WWW Document]. Dallas Morning News. URL http://crimeblog.dallasnews.com/2015/06/judge-rules-explosive-on-pipeline-in-plano-was-terrorism.html/

Wildavsky, A., Dake, K., 1990. Theories of risk perception: Who fears what and why? Daedalus 119, 41–60. doi:10.2307/20025337

Wooldridge, J.M., 2004. Introductory Econometrics, 2nd ed. South-Western.